DISEÑO DE PROPUESTA DE UNA GUIA PARA LA IMPLEMEMENTACION DE UN MODELO DE ARQUITECTURA EMPRESARIAL EN LOS ENTES DE CONTROL DEL ESTADO COLOMBIANO PARA LA GESTION ESTRATEGICA DE RIESGOS DE TI

NANCY MARIA PINTO RAMIREZ

MILEIDIS CAÑON CASTILLEJO

FUNDACIÓN UNIVERSITARIA DEL NORTE

MAESTRÍA EN GOBIERNO DE TI

BARRANQUILLA – ATLANTICO

2017

DISEÑO DE PROPUESTA DE UNA GUIA PARA LA IMPLEMEMENTACION DE UN MODELO DE ARQUITECTURA EMPRESARIAL EN LOS ENTES DE CONTROL DEL ESTADO COLOMBIANO PARA LA GESTION ESTRATEGICA DE RIESGOS DE TI

NANCY MARIA PINTO RAMIREZ

MILEIDIS CAÑON CASTILLEJO

Proyecto de Grado para optar por el Título de Magister en Gobierno de Tecnología De La Información

Director de Proyecto de Grado

Jorge Alberto Gil Peñaloza. MSc. MBA.

FUNDACIÓN UNIVERSITARIA DEL NORTE

MAESTRÍA EN GOBIERNO DE TI

BARRANQUILLA – ATLANTICO

2017

Nota de aceptación

Firma Presidente del Jurado

Firma Jurado 1

Firma Jurado 2

Ciudad: _____

Fecha: _____

Doy gracias a Dios, mis padres, mi hijo, Tomas, al cuerpo docente y administrativo de la universidad y a todas las personas que han estado a mi lado para apoyarme y hacer posible este sueño.

Nancy

Primero gracias a Dios, a Mis padres y Nestor que han sido un apoyo invaluable en el cumplimiento de esta meta, a mis compañeros y profesores que me dejaron grandes enseñanzas.

Mileidis

AGRADECIMIENTOS

A Dios primero que todo, al Dr. Jorge Alberto Gil Peñaloza nuestro tutor quien nos orientó durante el desarrollo de este trabajo.

A cada uno de los servidores y funcionarios de la Fiscalía General de la Nación que nos colaboraron para la elaboración de este proyecto.

RESERVA INFORMACION

Este documento es elaborado solo con fines educativos para la obtención del grado de Maestría en Gobierno de Tecnologías de la Información y toda la información allí suministrada de la entidad pública sobre la cual realizamos el trabajo de campo es de uso exclusivamente para consultas académicas y de consulta y revisión por parte de los jurados, tutor, profesores y demás personas participantes en este proceso. Así mismo, se deja claro que este documento, por contener información confidencial, sólo se dará a conocer para fines académicos y los conceptos y opiniones tratados y consignados en este trabajo no comprometen a ningún servidor y/o funcionario de la Fiscalía General de la Nación y son de total autoría de sus creadores solo para los intereses académicos ya anotados. En el evento de que alguno de sus lectores asocie su contenido con alguna entidad en particular, será producto de su libre entender, por lo que sus autores no se hacen responsables de ello. La información contenida en este documento es confidencial, empleada para fines únicamente académicos, de propiedad de sus autores, y no podrá usarse sin su autorización expresa.

UNIVERSIDAD DEL NORTE
ACREDITADA INSTITUCIONALMENTE POR SU EXCELENCIA ACADEMICA

Tabla de contenido

GLOSARIO

ARQUITECTURA EMPRESARIAL - AE: es una práctica estratégica que consiste en analizar integralmente a las entidades o instituciones desde diferentes perspectivas o dimensiones, con el propósito de obtener su estado actual y la visión a largo plazo, permitiendo alinear la estrategia, los procesos, los datos, y las aplicaciones e infraestructura tecnológica, con el fin de agregar valor a las organizaciones. En general, dentro de la Arquitectura Empresarial se identifican cuatro componentes, pero para el caso colombiano son seis: Estrategia, Gobierno de TI, Información, Sistemas de Información, Servicios de Tecnología y Uso y Apropiación. Su principal objetivo es garantizar la correcta alineación de la tecnología y los procesos de negocio en una organización, con el propósito de alcanzar el cumplimiento de sus objetivos estratégicos. [2][10]

PRINCIPIOS: El Marco de Referencia de Arquitectura Empresarial (AE) para la gestión de Tecnologías de la Información del Estado colombiano, se desarrollará con fundamento en los principios consagrados en los Artículos 209 de la Constitución Política, 3° de la Ley 489 de 1998 y 3° de la Ley 1437 de 2011.

BASE DE CONOCIMIENTO: provee un portafolio de instrumentos y herramientas que guían y ayudan a la implementación del Marco de Referencia de AE e incluye entre otros: estándares, lineamientos, guías, modelo de gestión de TI, mejores prácticas, soluciones y casos de éxito.

GUIA: definición procedimental que detalla por medio de actividades los pasos que debe ejecutar una entidad para producir un resultado. Provee las instrucciones de cómo adoptar/adaptar el estándar en lo que es aplicable a una entidad/sector. Una guía puede ser un instructivo, procedimiento, lista de verificación, una formulación, o modelo matemático o manual. Existen Guías referenciadas y Guías desarrolladas cuya diferencia es si existen o se proponen a partir de un estudio previo.

MARCO DE REFERENCIA COLOMBIANO: Es el principal instrumento para implementar la Arquitectura TI de Colombia y habilitar la Estrategia de Gobierno en línea. Con él se busca habilitar las estrategias de TIC para servicios, TIC para la gestión, TIC para el gobierno abierto y para la Seguridad y la privacidad.

INTEROPERABILIDAD: La interoperabilidad es la acción, operación y colaboración de varias entidades para intercambiar información que permita brindar servicios en línea a los ciudadanos, empresas y otras entidades mediante una sola venta de atención o un solo punto de contacto.

ARQUITECTURA TERRITORIAL: Es el análisis integral y estratégico de las oportunidades de desarrollo del territorio, incluidos el departamento, los municipios y las instituciones prestadoras de los servicios, basado en el Marco de Referencia.

ARQUITECTURA SECTORIAL: Al hablar de Arquitectura TI para los sectores públicos, se refiere al análisis integral y estratégico basado en el Marco de Referencia y en que los planes o estrategias deben estar alineados para garantizar que la tecnología otorga valor.

USO Y APROPIACIÓN: La gente involucrada en la gestión pública debe estar capacitada para tal labor. Al definir la Arquitectura TI de Colombia, se requiere una estrategia que les facilite a los funcionarios de las entidades utilizar la tecnología como motor de desarrollo. Esta estrategia incluye jornadas de sensibilización, capacitación, prácticas, recursos digitales, interacción con expertos y, en general, una amplia movilización para que la mayor cantidad posible de personas haga parte del proceso de desarrollo de la Arquitectura TI de Colombia.

ARQUITECTURA EMPRESARIAL ACTUAL (AS-IS): Es el análisis de la situación actual de la entidad u organización a partir de los dominios: (Negocio, Estrategia TI,

Gobierno TI, Información, Sistemas de Información, Servicios Tecnológicos y Uso y Apropiación).

ARQUITECTURA DE SOLUCIÓN: Cuando aparece un nuevo requerimiento que afecta varios sistemas de información o varias arquitecturas, se elabora una arquitectura de solución, que define la manera en que se deben ajustar las arquitecturas actuales (información, servicios tecnológicos y sistemas de información) para resolverlo. Esta arquitectura de solución debe respetar las arquitecturas de referencia existentes. Garantiza que los problemas se resuelven con una visión amplia y de alto nivel, y que se tiene en cuenta el impacto de las decisiones que se toman.

ANÁLISIS DE BRECHA: Se refiere a la identificación, comparación y análisis de las diferencias entre un estado o situación actual y el estado o situación deseada. Permite planear las arquitecturas de transición necesarias para implementar y alcanzar la arquitectura empresarial objetivo.

COSTO DE OPERACIÓN (OPEX): Hace referencia a los costos causados por la operación de una entidad, asociados a actividades que no producen valor de manera directa sino a actividades secundarias de apoyo.

DOMINIO: Cada uno de los seis componentes que conforman la estructura de la primera capa del diseño conceptual del Marco de Referencia de Arquitectura Empresarial para la gestión de TI. Los dominios son las dimensiones desde las cuales se debe abordar la gestión estratégica de TI. Agrupan y organizan los objetivos, áreas y temáticas relativas a las TI.

DERECHOS PATRIMONIALES: Son los derechos de índole económica, que implican para su titular la facultad de autorizar o prohibir la explotación de la obra o creación.

ESTRATEGIA TI: Es el conjunto de principios, objetivos y acciones concretas que reflejan la forma en la cual una entidad decide utilizar las Tecnologías de la Información para permitir el logro de su misión de una manera eficaz. La Estrategia TI es una parte integral de la estrategia de una entidad.

FUNCIÓN: Responsabilidad o actividad inherente a un rol.

GOBIERNO DE TI: Es una práctica, orientada a establecer unas estructuras de relación que alinean los procesos de negocio con los procesos, recursos y estrategias de TI, para agregar valor a las organizaciones y apoyar el cumplimiento de sus objetivos estratégicos. El gobierno de TI, gestiona y controla los riesgos, mide el desempeño de TI, busca optimizar las inversiones de TI y establecer un esquema de toma de decisiones de TI. El gobierno de TI, es parte del gobierno corporativo o empresarial.

GESTIÓN DE TI: Es una práctica, que permite operar, innovar, administrar, desarrollar y usar apropiadamente las tecnologías de la información (TI), con el propósito de agregar valor para la organización. La gestión de TI permite a una organización optimizar los recursos, mejorar los procesos de negocio y de comunicación y aplicar las mejores prácticas.

HERRAMIENTAS: Mecanismos que les permiten a las instituciones materializar acciones específicas asociadas con directrices dadas por el Marco de Referencia de Arquitectura Empresarial para la Gestión TI, específicamente por un lineamiento o una guía. Las herramientas son identificadas y referenciadas con base en las mejoras prácticas de TI para apoyar la arquitectura y la gestión.

MECI: Modelo Estándar de Control Interno para el Estado Colombiano – MECI - proporciona la estructura básica para evaluar la estrategia, la gestión y los propios mecanismos de evaluación del proceso administrativo, y aunque promueve una

estructura uniforme, puede ser adaptada a las necesidades específicas de cada entidad, a sus objetivos, estructura, tamaño, procesos y servicios que suministran.

El MECI concibe el Control Interno como un conjunto de elementos interrelacionados, donde intervienen todos los servidores de la entidad, como responsables del control en el ejercicio de sus actividades; busca garantizar razonablemente el cumplimiento de los objetivos institucionales y la contribución de éstos a los fines esenciales del Estado; a su vez, persigue la coordinación de las acciones, la fluidez de la información y comunicación, anticipando y corrigiendo, de manera oportuna, las debilidades que se presentan en el quehacer institucional.

METODOLOGÍA DE REFERENCIA: Es un conjunto de técnicas, etapas, actividades, patrones y artefactos que plantean una manera disciplinada y organizada de abordar un problema en un contexto específico. Resume la experiencia y las mejores prácticas de los expertos en un tema. Es una metodología ampliamente difundida y utilizada, usualmente respaldada por algún tipo de organización nacional o internacional.

NORMATIVIDAD: Leyes, decretos y demás desarrollos normativos que guían las acciones para implementar el Marco de Referencia de Arquitectura Empresarial para la gestión de TI.

PUNTO DE VISTA ARQUITECTURAL: Una arquitectura, en general, es el conjunto de estructuras que constituyen un sistema. Cada una tiene, entre otras cosas, un grupo de componentes y sus relaciones. Un punto de vista de una arquitectura es un subconjunto de componentes y relaciones, provenientes de una o varias estructuras, con un significado o interés particular dentro del sistema. Una vista es el cálculo de un punto de vista sobre una arquitectura específica. En el caso del Marco de Referencia de Arquitectura Empresarial para la gestión de Tecnologías de la Información se construyeron cuatro puntos de vista arquitecturales: (1) punto de

vista del país, (2) punto de vista estructural de una institución, (3) punto de vista de transformación de una organización y (4) punto de vista metodológico.

PLAN DE COMUNICACIÓN DE LA ESTRATEGIA DE TI: Toda estrategia debe ser comunicada de manera adecuada a los distintos interesados, dentro y fuera de una institución. El plan de comunicación define los tipos de usuarios a los que se informará, los tipos de contenido y medios de comunicación por usar, para divulgar la Estrategia de TI. Este plan es uno de los componentes de un PETI (Plan Estratégico de TI).

POLÍTICA DE TI: Es una directriz u orientación que tiene el propósito de establecer pautas para lograr los objetivos propuestos en la Estrategia de TI. Las políticas son usadas para dirigir las decisiones, para asegurar la consistencia y el apropiado desarrollo e implementación de los procesos, estándares, roles, actividades y servicios de TI.

PETI: El Plan Estratégico de las Tecnologías de la Información y Comunicaciones es el artefacto que se utiliza para expresar la Estrategia de TI. Incluye una visión, unos principios, unos indicadores, un mapa de ruta, un plan de comunicación y una descripción de todos los demás aspectos (financieros, operativos, de manejo de riesgos, etc.) necesarios para la puesta en marcha y gestión del plan estratégico. El PETI hace parte integral de la estrategia de la institución. Cada vez que una entidad hace un ejercicio o proyecto de Arquitectura Empresarial, su resultado debe ser integrado al PETI.

PLAN DE CAPACITACIÓN Y ENTRENAMIENTO: Define las actividades de capacitación y entrenamiento que se requieren para entrenar a los funcionarios de una entidad en aspectos específicos de una aplicación, una metodología, un producto, una tecnología o un proceso.

VALOR: En un contexto organizacional, generar y entregar valor significa, en general, proveer un conjunto de servicios y productos para facilitarle a alguien el logro de un objetivo. TI genera y entrega valor a una institución mediante la implementación de los servicios de TI. La entrega de valor es una medida abstracta, difícil de cuantificar directamente, pero que se puede calcular con el ahorro en esfuerzo o el aumento en la calidad del objetivo institucional que apoya.

VISIÓN ESTRATÉGICA: Es la definición de alto nivel de los objetivos que se pretenden lograr y de la manera de hacerlo. Es uno de los componentes del PETI. En el caso de TI, la visión estratégica debe contemplar el impacto de las nuevas tecnologías, los cambios en las necesidades y expectativas de los ciudadanos, usuarios y actores de la entidad.

RESUMEN

El presente documento propone el diseño de una guía para la implementación de un modelo de AE para entidades del estado colombiano para la gestión estratégica de riesgos de TI, que pueda servir de base para aplicar a cualquier ente de control. Fue realizado tomando como referencia la Fiscalía General de la Nación en Colombia. Se propone una guía como complemento de la establecida por MINTIC Colombia en su modelo de AE, resaltando que en esta guía los riesgos de TI deben ser transversales a todos los dominios y en todos los procesos existentes en la entidad. De esta manera se alcanzara un nivel significativo de madurez, alineando los procesos, los datos, las aplicaciones y tecnología con los objetivos estratégicos con el fin de mejorar sus niveles de productividad.

Palabras Claves: Arquitectura Empresarial, entidades del estado, Tecnologías de la Información, Gobierno de IT, Riesgos de TI.

ABSTRACT

This document proposes the design of guidelines for the implementation of a model of AE for entities of the Colombian State for strategic management of risk, which can serve as a basis to apply to any body control. It was made with reference to the Office of the Attorney-General in Colombia. Proposes a guide to complement established by MINTIC Colombia in its AE model, emphasizing that in this guide the risk must be transversal to all domains and all processes existing in the State. In this way reached a significant level of maturity, aligning processes, data, applications, and technology with strategic objectives in order to improve their productivity.

Keywords: Enterprise architecture, institutions of the State, information technology, Government of IT, risk.

INTRODUCCION

Este documento compila información relacionada con la situación actual de los proyectos, procesos, procedimientos y actividades que deben ser implementando en la Fiscalía General de la Nación para cumplir con lo establecido en el decreto 415 del 07 de marzo de 2016, por medio del cual se adiciona el Decreto Único Reglamentario del sector de la Función Pública, Decreto Numero 1083 de 2015, en lo relacionado con la definición de los lineamientos para el fortalecimiento institucional en materia de tecnologías de la información y las comunicaciones.

Es por eso que se identifican y muestra las necesidades que en materia de tecnología posee la FGN y se complementa la guía de evidencia establecida por MINTIC para la implementación de AE en la entidades del estado, agregando los riesgos de TI para análisis transversal en cada uno de los dominios planteados, generando mejores alternativas de solución, teniendo en cuenta que los Riesgos de TI deben ser analizados por todos los procesos existentes en la entidad, lo anterior teniendo en cuenta los lineamientos para el fortalecimiento institucional y el cumplimiento de los objetivos estratégicos.

Con la implementación del modelo de AE establecido por MINTIC para las entidades del estado , la Fiscalía General de la Nación permitirá un mejor acceso a la administración de justicia, por parte de los ciudadanos, una justicia pronta y cumplida, unos trámites eficientes y la gestión y el control de la operación del “negocio” de la FGN, motivaran el desarrollo de los pilares de infraestructura, comunicaciones, redes, seguridad y sistemas de información, para crear un ecosistema tecnológico que permita responder a los nuevos desafíos y demandas de los usuarios internos y externos.

1. FORMULACIÓN DEL PROBLEMA

1.1 ANTECEDENTES

El emergente proceso de digitalización y avance tecnológico originario de cambios en la sociedad moderna, es uno de los retos a enfrentar por las nacientes economías, así como por países en proceso de desarrollo, situación que no solamente afecta al sector productivo, en el entendido que trasciende al fragmento público el cual actúa como garante de actividades que no admiten libre comercialización y sobre las cuales recae el nacer tecnológico que pretende mantener un nivel de competitividad acorde con las exigencias de la realidad global.

Con este adelanto de las sociedades, nacen también nuevos procesos, los cuales se insertan en todos los componentes del entorno, incluyendo las organizaciones, vistas éstas como uno de los engranajes fundamental para el desarrollo social.

Una de las condiciones a enfrentar con ocasión de los procesos de cambio originados por la evolución del mundo globalizado, lo constituyen las tecnologías de la información, las cuales deslumbran cada día al presentar ideas que buscan la mejora continua en los sistemas que mueven el mundo; incluye esto a los gobiernos, los cuales deben mantenerse a la vanguardia de los avances, bien sea con fines de interacción con los integrantes del sistema o en su condición de solemnidad legitima de la sociedad.

Bajo los anteriores preceptos, el Estado Colombiano busca la implementación de estrategias con el fin de reducir la brecha originaria de desigualdades en criterios de acceso a las nuevas tecnologías de la información y las comunicaciones (TIC), así como la necesidad de ubicar a la Nación en los niveles de aceptación de su administración pública que permitan la interacción entre las administraciones de

países a nivel latinoamericano respecto al avance de las TIC en los países más desarrollados y con los particulares que sean vinculados en cualquier actividad pública.

Es así como en los inicios de los procesos de modernidad tecnológica, el gobierno colombiano mediante la creación de programas como *Gobierno en Línea*[1] señala el horizonte a tener presente para la puesta en funcionamiento del cambio hacia la modernización tecnológica y estratégica, mediante la adopción de buenas prácticas de administración pública.

En diciembre del año 2014, la legislación colombiana en concurso con el Estado, fue más allá y promulga el decreto 2573 *"por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en Línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones*".

El objeto es definir los parámetros, instrumentos y plazos de la estrategia de Gobierno en Línea para garantizar el máximo aprovechamiento de las Tecnologías de la Información y las Comunicaciones, con el fin de contribuir con la construcción de un Estado abierto, más eficiente, más transparente, más participativo y que preste mejores servicios con la colaboración de toda la sociedad.[2]

Es preciso señalar que las organizaciones hoy día enfrentan un entorno de funcionamiento y operatividad con altos niveles de complejidad, procesos dinámicos y enmarcados en un contexto de globalización, buscando además buenos niveles de competitividad. Sumado a lo anteriormente expuesto, las empresas deben manejar la complejidad de su información y la tecnología, y mantener activos los

[1] Gobierno en línea es el nombre que recibe la estrategia de gobierno electrónico (e-government) en Colombia, que busca construir un Estado más eficiente, más transparente y más participativo gracias a las TIC.

[2] Decreto 2573 de 2014, diciembre 12.

sistemas y el ambiente computacional que vienen operando desde años atrás, pero también, con la necesidad de afrontar los retos que día a día le impone el negocio para apoyar su operación. [1] El entendimiento de la complejidad que afrontan las organizaciones, resulta ser el punto de partida para las relaciones del negocio; conocer de lleno los procesos y la posición en la cadena de producción de bienes o servicios se logra mediante la imposición del concepto y andamiaje conocido como Arquitectura Empresarial (AE), el cual ha emergido a comienzos de los 90.

Es así como se fija la necesidad en cabeza del Ministerio de Tecnologías de la Información y las Comunicaciones de implementar un Marco de Referencia de Arquitectura Empresarial para la gestión de Tecnologías de la Información del Estado Colombiano, el cual se fundamenta además en los principios constitucionales artículo 209 de la constitución política de Colombia, 3° de la Ley 489 de 1998 y 3° de la Ley 1437 de 2011, decreto 415 de 2016.

Esta iniciativa fue ratificada por el Gobierno Colombiano y su pretensión se plasma en la definición de un modelo de Arquitectura Empresarial para la gestión de TI en el Estado, mediante el cual se busca que las entidades públicas del orden nacional puedan crear entre si niveles de articulación buscando efectividad y eficiencia en la prestación de servicios a nivel interno y externo. No obstante, no existe una guía que permita implementar en la práctica dicho modelo en las entidades del Estado Colombiano, la cual tome como fundamento, entre otros aspectos, los modelos existentes y se ajuste a las particularidades, para el caso de este trabajo, de las entidades de control que lo conforman.

Es preciso recordar que la Arquitectura Empresarial- AE: es una práctica estratégica que consiste en analizar integralmente a las entidades o instituciones desde diferentes perspectivas o dimensiones, con el propósito de obtener su estado actual y la visión a largo plazo, permitiendo alinear la estrategia, los procesos, los datos, aplicaciones e infraestructura tecnológica, con el fin de agregar valor a las

organizaciones. En general, dentro de la Arquitectura Empresarial se identifican cuatro componentes (Arquitectura de negocio, de información, de aplicación y arquitectura tecnológica), pero para el caso colombiano son seis: Estrategia, Gobierno de TI, Información, Sistemas de Información, Servicios de Tecnología y Uso y Apropiación. Su principal objetivo es garantizar la correcta alineación de la tecnología y los procesos de negocio en una organización, con el propósito de alcanzar el cumplimiento de sus objetivos estratégicos. [2]

El anterior concepto vincula además: 1) La Arquitectura de Negocio, la cual se concibe como un componente de la arquitectura empresarial en el que se define la misión, visión, servicios, estrategia, procesos, organización y regulación que debe cumplir la entidad, además de los flujos de información e información que se necesita para alcanzar sus objetivos misionales, y 2) La Arquitectura Empresarial de TI, que es un componente de la arquitectura empresarial en el que se definen vistas lógicas de información, sistemas de información, infraestructura, servicios tecnológicos y un ambiente de gestión de TI para contribuir con la transformación empresarial. Este concepto que liga las pretensiones de Administración del Negocio y Gobierno de TI, tiene especial importancia al ser integrado dentro de las organizaciones modernas con el objeto de mejorar los usos de las tecnologías de información y las comunicaciones (TIC) en las mismas, lo que será producto de la correcta implementación del modelo acorde a cada una de las necesidades de la entidad.A partir de estos conceptos muy generales, se propone entonces el diseño de una propuesta de guía para la implementación de un modelo de Arquitectura Empresarial, específicamente, para los entes de control del Estado Colombiano, con aplicación piloto en uno de ellos, para la gestión estratégica de riesgos de TI, que buscará contribuir al cumplimiento las nuevas exigencias jurídicas para el caso requerido y a minimizar la ocurrencia de eventos en contra de la administración pública.

1.2 PLANTEAMIENTO DEL PROBLEMA

La gestión de riesgos en el área de TI resulta de vital importancia para el desarrollo del rol empresarial, es una alternativa utilizada por muchas empresas y la tendencia de la formulación de estos está en crecimiento. Su implementación no garantiza una total cobertura para las dependencias de las entidades y en especial para el área de tecnologías de información, de sus responsabilidades como garante del proceso de gestión de información, por lo que **se requiere que las entidades establezcan un direccionamiento alineado con la estrategia de negocio y la aplicación de nuevas prácticas de gobierno y gestión para el manejo de los mismos**, por lo anterior **se propone el diseño de una guía para la implementación de un modelo de arquitectura empresarial en la Fiscalía General de la Nación para la gestión de riesgos de TI**. La cual servirá como caso de éxito para otras entidades del estado colombiano.

1.3. JUSTIFICACIÓN

El ministerio de tecnologías de la información y de las comunicaciones sentó las bases mediante la formulación del marco de referencia de Arquitectura Empresarial para las instituciones del Estado Colombiano; tendiente a ser utilizado como orientador estratégico de sus arquitecturas empresariales, tanto sectoriales como institucionales.

El Marco es un modelo mediante el cual se establece la estructura conceptual, define lineamientos, propone la incorporación de mejores prácticas y traza una ruta de implementación para lograr una administración pública más eficiente, coordinada y transparente, a través del fortalecimiento de la gestión de las TI de las instituciones.

Esta intención del Estado Colombiano es apoyada por cada sector integrante del mismo, es así como resulta indispensable que las instituciones para el cumplimiento

de los objetivos propuestos se ven en la necesidad de diseñar e implementar el modelo de Arquitectura Empresarial que será acorde a los intereses de cada una de ellas.

El modelo presentado se elabora sobre lo propuesto por MINTIC profundizando en la gestión de riesgos de TI a través de la implementación de un modelo de arquitectura empresarial aplicable a un ente de control del Gobierno Colombiano.

2. OBJETIVOS

2.1 OBJETIVO GENERAL

Como pilar de las buenas prácticas y herramientas que hacen viable el Gobierno de TI, se propone el diseño de una propuesta de guía para la implementación de un modelo de Arquitectura Empresarial en los entes de control del Estado Colombiano para la gestión estratégica de riesgos de TI, utilizando como referencia diferentes modelos y marcos de trabajo, entre ellos, de arquitectura empresarial, TOGAF, ZACHMAN y el modelo propuesto por el gobierno a través del ministerio de tecnologías y las comunicaciones, así como de gestión de riesgos de Cobit 5.0 e ISO31000.

2.2 OBJETIVOS ESPECIFICOS

1. (Fase 1 – Diagnóstico) Establecer el marco referencial y estudiarlo en detalle a partir de: a) documentación existente (marcos de trabajo, metodologías y buenas prácticas existentes en la literatura sobre el tema), b) antecedentes, contexto y avances en materia de desarrollo de este tipo de herramientas en entidades de control del Estado Colombiano, y c) experiencia de las autoras de este trabajo.

2. (Fase 2 – Especificación) A partir de los resultado de la fase 1 (objetivo específico 1):

   2.1 Definir los requerimientos básicos para el desarrollo de la guía de implementación.

2.2 Extraer del estudio realizado en la fase 1, los componentes y experiencias que aplicarían en mayor grado como fundamento para el diseño de la guía propuesta de implementación de un modelo de Arquitectura Empresarial para el contexto de gestión de riesgo de TI en entes de control.

3. (Fase 3. Construcción) Diseñar y documentar la guía propuesta a partir del resultado de la fase 2. La guía constará de una serie de sub fases para las que se especificarán las entradas y salidas de cada una, así como las actividades a realizar dentro de ellas, aplicando los productos de la fase 2.

4. (Fase4. Presentación de una propuesta de Implementación) como trabajo de campo, presentar y proponer la guía a un ente de control del Estado Colombiano.

3. ALCANCE Y LIMITACIONES

3.1 ALCANCE

El proyecto se desarrollará tomando como referencia la investigación de la literatura y experiencias existentes, y se llevará a cabo un análisis detallado de cada aspecto relevante para el diseño de una propuesta de guía para la implementación de un modelo de Arquitectura Empresarial en los entes de control del estado colombiano para la gestión estratégica de riesgos de TI. Luego se realizará una propuesta que será entregada a una seccional del ente de control del Estado Colombiano. Se espera que esta presentación sirva de punto de partida para iniciar un proyecto de implementación piloto que permita depurar la guía y hacerla práctica para toda la entidad. El ente seleccionado y la seccional son del Cesar: Dirección de Control Interno, de la Fiscalía General de la Nación. No es alcance de este trabajo la realización de dicho proceso ni la posterior, si es exitoso el piloto, replicación y aplicación en las demás seccionales o, con las debidas adaptaciones, en otras entidades de control del Estado.

3.2 LIMITACIONES

El documento final será una propuesta de guía para la implementación de un modelo de AE general de TI para las entidades de control del Estado Colombiano (presentada y propuesta a una de ellas), que podría ser tomada como base, para ser posteriormente revisada y ajustada, y poder ser aplicada por otras entidades de control del Estado. La aplicación (implementación real como trabajo de campo) de la presente investigación y diseño del modelo está limitado a la gestión de riesgos de TI en entes de control del Estado Colombiano, y se presentará a una Seccional como propuesta de un proyecto piloto, más no puede ser asumida como una guía definitiva. Lo anterior, dado que se encuentra fuera del alcance la implementación definitiva de la misma en todas las áreas de un ente de control, en el entendido que

debe superar la aprobación de diferentes instancias de alto nivel y la guía debería ser sometida a criterios de evaluación educativa y su implementación definitiva implicaría la aceptación por parte del Estado Colombiano como un todo.

4. MARCO TEÓRICO

4.1 Arquitectura Empresarial

Una de las disciplinas de la informática que mayor peso ha cobrado en los últimos años es la Arquitectura Empresarial (AE, en inglés 'Enterprise Architecture'), que puede explicarse en función de las metas de una organización y en cómo desde los sistemas se pueden proponer formas de organizar sus procesos para optimizar los recursos y lograr así los objetivos propuestos.

"La Arquitectura Empresarial es una metodología que, basada en una visión integral de las organizaciones – o en este caso, de todo el Estado –, permite alinear procesos, datos, aplicaciones e infraestructura tecnológica con los objetivos estratégicos del negocio o con la razón de ser de las entidades. (...) Su principal objetivo es garantizar la correcta alineación de la tecnología y los procesos de negocio en una organización, con el propósito de alcanzar el cumplimiento de sus objetivos estratégicos". [3]

Una entidad que desarrolle su AE logra dejar de lado las preocupaciones por los aparatos, el flujo de información y hasta la instalación de nuevos sistemas informáticos, para ocuparse de tomar decisiones basadas en la mayor cantidad de información disponible, básicamente porque el papel de la Arquitectura es definir lineamientos informáticos que resuelvan las necesidades actuales y prevean las futuras en función de la toma de decisiones, es decir, proponiendo formas de generar bases de datos integradas, generando estándares de desarrollo de aplicaciones y servicios internos para que sean compatibles y puedan compartir información entre ellos, e incluso dando marcos de referencia para la compra y disposición de equipos informáticos, así como de disposición del recurso humano necesario para cada uno de los puntos en interacción.

Según el Centro de Formación de IBM, el papel del arquitecto de información, más allá de manejar las metodologías y generar los mapas de procesos que delinearán las rutas tecnológicas a seguir por todas las áreas de la entidad, es "describir los componentes de una empresa, sus relaciones, cómo colaboran e interactúan entre sí con el 'mundo exterior'. Una Arquitectura Empresarial ofrece la orientación para implantar los componentes de la empresa. La implantación de los componentes produce un cambio en el estado de la empresa". [4]

4.1.1 Componentes de la Arquitectura Empresarial

El secreto de la AE radica en la alineación de los distintos componentes informáticos de una organización, todos en función de una visión estratégica que les dé sentido y, a la vez, que los convierta en recursos útiles para la toma de decisiones, más allá del conjunto de recursos para realizar tareas en que pueden convertirse sin una integración desde la Arquitectura.

"En general, dentro de la Arquitectura Empresarial se identifican seis componentes: estrategia, gobierno de TI, información, sistemas de información, servicios de tecnología, uso y apropiación". [5]

Amazing Colombia, firma consultora en AE, presenta estos componentes de la siguiente manera:

Figura 1. Componentes de la Arquitectura Empresarial.
Fuente: http://cintel.co/wp-content/uploads/2013/05/por-que-arquitectura-empresarial.pdf

Las organizaciones que se dan a la tarea de desarrollar su AE logran, entre otras, que ésta "apoye el cumplimiento de los objetivos estratégicos, garantizando que las iniciativas planteadas correspondan a programas/proyectos que den solución a los requerimientos y necesidades de negocio" (Amazing Consultores).

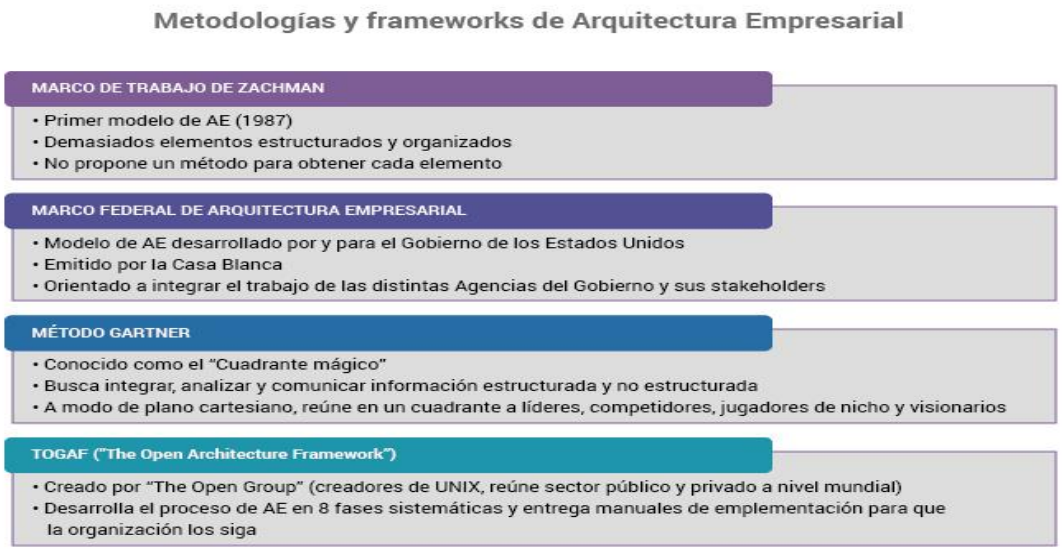
Este gran logro es aún más comprensible al considerar que "el marco de planeación del negocio (planeación prospectiva, estratégica, por objetivos, balanced scorecard, etc.) define la estrategia y objetivos del negocio, da dirección, es el 'qué', mientras que la AE establece el 'cómo', definiendo las capacidades de construir, la lógica organizativa y los recursos necesarios", tal como lo indica CINTEL en el documento '¿Por qué Arquitectura Empresarial?'. [6]

4.1.2 Desarrollo de una Arquitectura Empresarial, Metodologías y 'Frameworks'.

Considerando que el núcleo del logro de la AE está en su capacidad de alineación entre todos los sistemas y procesos de la organización, es apenas lógico pensar que existen metodologías estándar diseñadas con el propósito de desarrollar la Arquitectura y permitir, entre otras, que los desarrolladores puedan generar propuestas que se integren con facilidad a la misma.

De acuerdo con el consultor Jorge Londoño, los 'frameworks' son necesarios porque "agilizan y simplifican la definición y el desarrollo de la Arquitectura, asegurando un cubrimiento más completo de la solución diseñada; aseguran que la Arquitectura seleccionada permita un crecimiento futuro en respuesta a las necesidades del negocio; porque diseñar una Arquitectura es un proceso técnicamente complejo y el diseño de arquitecturas heterogéneas de múltiples proveedores es particularmente complejo; y porque (con ellos) se desmitifica la AE".

Existen cuatro metodologías o marcos de trabajo ('frameworks') de alto reconocimiento para desarrollar la AE:



Fuente: Desarrollo de Colombia Digital a partir de múltiples fuentes

4.2. Arquitectura Empresarial en el contexto de TOGAF

TOGAF es una de las metodologías más populares para desarrollar AE, pues permite planificar, diseñar, evaluar e implementar la arquitectura empresarial de información en una organización.

"TOGAF es una herramienta para asistir en la aceptación, creación, uso, y mantenimiento de arquitecturas. Está basado en un modelo iterativo de procesos apoyado por las mejores prácticas y un conjunto reutilizable de activos arquitectónicos existentes", según la 'Guía de bolsillo TOGAF V. 9.1.1'.[7]

La Arquitectura Empresarial busca optimizar los procesos que apoyan la realización de la estrategia de negocio en toda la organización. Actualmente, los empresarios están al tanto que las tecnologías de información son claves para el éxito de los negocios.

4.2.1 Componentes de la Arquitectura Empresarial en el contexto de TOGAF

TOGAF beneficia a las organizaciones que necesitan un flujo de información continúo, donde los sistemas de información son un obstáculo para la operación y que buscan habilitar el cambio estratégico del negocio, convirtiendo las TI en un elemento estratégico de negocio.

La Arquitectura Empresarial se enfoca en hacer más productiva y competitiva una organización a través del uso de la tecnología como herramienta de ejecución e integración de sus procesos.

Desarrollado en 1995 y mantenido por el Foro de Arquitectura de The Open Group, **esta arquitectura está diseñada en cuatro niveles o dimensiones que son comúnmente aceptados como un subconjunto de una arquitectura empresarial.**

1- Arquitectura de Negocio: Identifica la cadena de valor de la organización desde macro hasta subprocesos. Dicha identificación pasa por las áreas de cadena de producción de valor (procesos de negocio CORE), áreas de procesos de dirección y áreas de soporte administrativo.
Tras la identificación, pasa entonces a la Definición de la Arquitectura de Procesos de Negocio.

Usa BPMN (Business Process Modeland Notation) como técnica de modelamiento para proveer una notación estándar fácilmente leíble y entendible para los involucrados en el negocio, como lo son los analistas de negocio, los desarrolladores técnicos y los gerentes y administradores del negocio.

BPMN sirve como lenguaje común entre las partes para un entendimiento comunicacional factible que frecuentemente se presenta entre el diseño de los procesos de negocio y su implementación.

2- Arquitectura de Datos: Establece el modelo de gestión de todos los aspectos del ciclo de vida de la información, es decir, identifica el modelo de Entidades de Negocio y su relación con los procesos de negocio buscando así la forma de crear, almacenar, mover, utilizar y retirar los datos.

3- Arquitectura de Aplicación: Identificar la Arquitectura Empresarial de Aplicaciones actual de la organización a través del levantamiento oficial del catálogo de aplicaciones actuales, la identificación de iniciativas en ejecución, y un análisis de cubrimiento de estas aplicaciones en los procesos de negocio.
Luego se plantea la Arquitectura Empresarial de Aplicaciones objetivo, basada en marcos de referencia y mejores prácticas de la industria. Este planteamiento contempla un acercamiento al modelo de integración que debe tener la Arquitectura Empresarial de Aplicaciones.

Tras estos procesos y con los resultados de la Arquitectura de Procesos, Datos y Aplicaciones, se plantea entonces la definición conceptual de una “Arquitectura SOA”, que se basa en la especificación de los servicios y su distribución en cada una de las 6 capas de Arquitectura SOA (capa de soluciones, capa de procesos, capa de lógica de negocio, capa de servicios core, capa de aplicativos, capa de utilities) a fin de garantizar sus requerimientos de implementación de acuerdo a su función dentro de la Arquitectura SOA.

4- Arquitectura Tecnológica: Validar las capacidades de software y hardware que se requieren para apoyar la implementación de servicios de negocio, datos y aplicación. Esto incluye infraestructura de IT, capa de mediación, redes, comunicaciones, procesamiento y estándares.

Para esto se ejecutan los siguientes pasos:

- Seleccionar los modelos de referencia y herramientas.
- Identificar la Arquitectura actual referente Hardware y Software de Plataforma.
- Desarrollar la descripción de la arquitectura objetivo Hardware y Software de Plataforma que cumpla con la visión de la Arquitectura Empresarial.
- Ejecutar el análisis de brecha e identificar los impactos que los cambios que se deban contemplar.
- Ejecutar una revisión formal por parte de los interesados y la toma de decisiones sobre adquisiciones, actualización y racionalización de elemento de tecnología.

TOGAF tiene un método de sentido común, efectivo, práctico y prudente para desarrollar la arquitectura empresarial y consiste de tres partes principales:

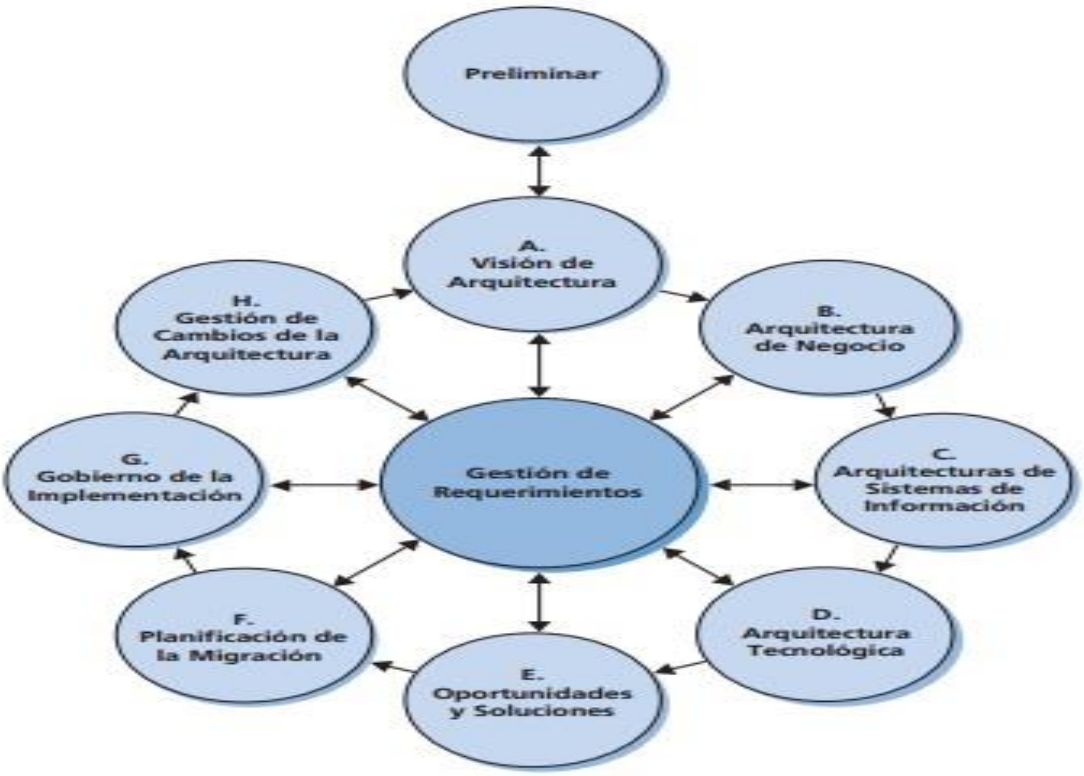


Figura 2. Componentes AE – TOGAF

Fuente: http://consultec-ti.com/blog/togaf-metodologia-mas-popular-para-desarrollar-arquitectura-empresarial/

4.2.1.1 Método para Desarrollar la Arquitectura

(ADM, por sus siglas en inglés). El ADM es el resultado de las contribuciones de numerosos profesionales de la arquitectura y constituye el núcleo de TOGAF. Es un método para obtener Arquitecturas Empresariales que son específicas para la organización, y está especialmente diseñado para responder a los requerimientos del negocio.

El ADM se prepara desde la fase preliminar que prepara a una organización para emprender proyectos de Arquitectura empresarial de manera exitosa.

ADM en detalle:

Fase preliminar:

Prepara a una organización para emprender proyectos de Arquitectura Empresarial de manera exitosa

a) Visión de la Arquitectura:

Aborda el establecimiento del proyecto e inicia una iteración del ciclo de desarrollo de la arquitectura, estableciendo el alcance, limitaciones y expectativas de la iteración. Se ejecuta con el objetivo de validar el contexto del negocio y producir una Declaración de Trabajo de Arquitectura aprobada.

b) Arquitectura de Negocio:

Aborda el desarrollo de negocio que apoye la visión de la arquitectura acordada.

c) Arquitecturas de sistemas de información:

Aborda la documentación de la organización fundamental de los sistemas de TI de una empresa, representada por los principales tipos de sistemas de información y aplicaciones que los utilizan.

d) Arquitectura tecnológica:

Aborda la documentación de la organización esencial de sistemas TI, representada en hardware, software y tecnología de comunicaciones.

e) Oportunidades y soluciones:

Esta fase se refiere a la implementación directamente. Describe el proceso de identificación de los medios de entrega (proyectos, programas o carteras) que proporcionan la Arquitectura de Destino identificada en las fases anteriores.

f) Planificación de la Migración:

Aborda la planificación de la migración, es decir, cómo moverse desde la Arquitectura de la Línea de Base a la Arquitectura de Destino, finalizando un plan de implementación y migración.

g) Gobierno de la Implementación:

La arquitectura delimita los proyectos de implementación, la supervisa al mismo tiempo que se la construye y produce un contrato de arquitectura firmado.

h) Gestión de Cambios de la Arquitectura:

Asegura que los cambios en la arquitectura se gestionen de manera controlada.

Gestión de Requerimientos:

Se aplica a todas las fases del ciclo del ADM. El proceso de Gestión de Requerimientos es un proceso dinámico que aborda la identificación de los requerimientos de la empresa, almacenándolos y luego gestionándolos al ingreso y egreso de las fases relevantes del ADM. Este proceso es fundamental para conducir el proceso del ADM.

La capacidad para hacer frente a los cambios de requerimientos es crucial para el proceso del ADM, pues la arquitectura, por su propia naturaleza, aborda la incertidumbre y el cambio, tendiendo un puente entre las aspiraciones de los interesados y lo que se puede entregar como una solución práctica.

El alcance del ADM debe ser determinado por la propia organización.

4.2.1.2 Continuum Empresarial: Repositorio de los activos de la arquitectura, modelos, patrones, descripciones, etc.
Proporciona un modelo para estructurar un repositorio virtual así como también métodos para clasificar artefactos de arquitectura y de solución, mostrando cómo los diferentes tipos de artefactos evolucionan, y cómo se pueden aprovechar y

reutilizarse. El Continuum de Empresa se basa en arquitecturas y soluciones que existen dentro de la empresa y la industria en general.

4.2.1.3 Recursos de TOGAF: El Marco de referencia de la Capacidad Arquitectónica es un conjunto de recursos, guías, plantillas, información general, étc., proporcionados para ayudar al arquitecto a establecer una práctica de arquitectura dentro de una organización. TOGAF refleja la estructura y el contenido de la capacidad arquitectónica dentro de una empresa. .[7].

4.3 Arquitectura Empresarial en el contexto de Zachman

El Marco de Trabajo Zachman es un framework de Arquitecturas empresariales creado por John A. Zachman en 1984 y publicado por primera vez en el IBM Systems Journal en 1987. Es uno de los marcos de trabajo más antiguos y de mayor difusión en la actualidad.

Zachman es en realidad una taxonomía arquitectónica, es decir, un esquema para organizar y categorizar artefactos arquitectónicos (documentos de diseño, especificaciones y modelos) que toma en cuenta tanto a quién está dirigido el artefacto como a cuál asunto particular está siendo orientado. Esto lo hace perfecto para documentar una Arquitectura de Sistemas de Información.
El propósito del marco de Zachman es proveer la estructura básica que soporta la organización, el acceso, la integración, la interpretación, el desarrollo, la administración y el cambio de un conjunto de representaciones (artefactos) arquitectónicas de los sistemas de información de la empresa. [8]

4.3.1 Componentes de la Arquitectura Empresarial en el contexto de Zachman

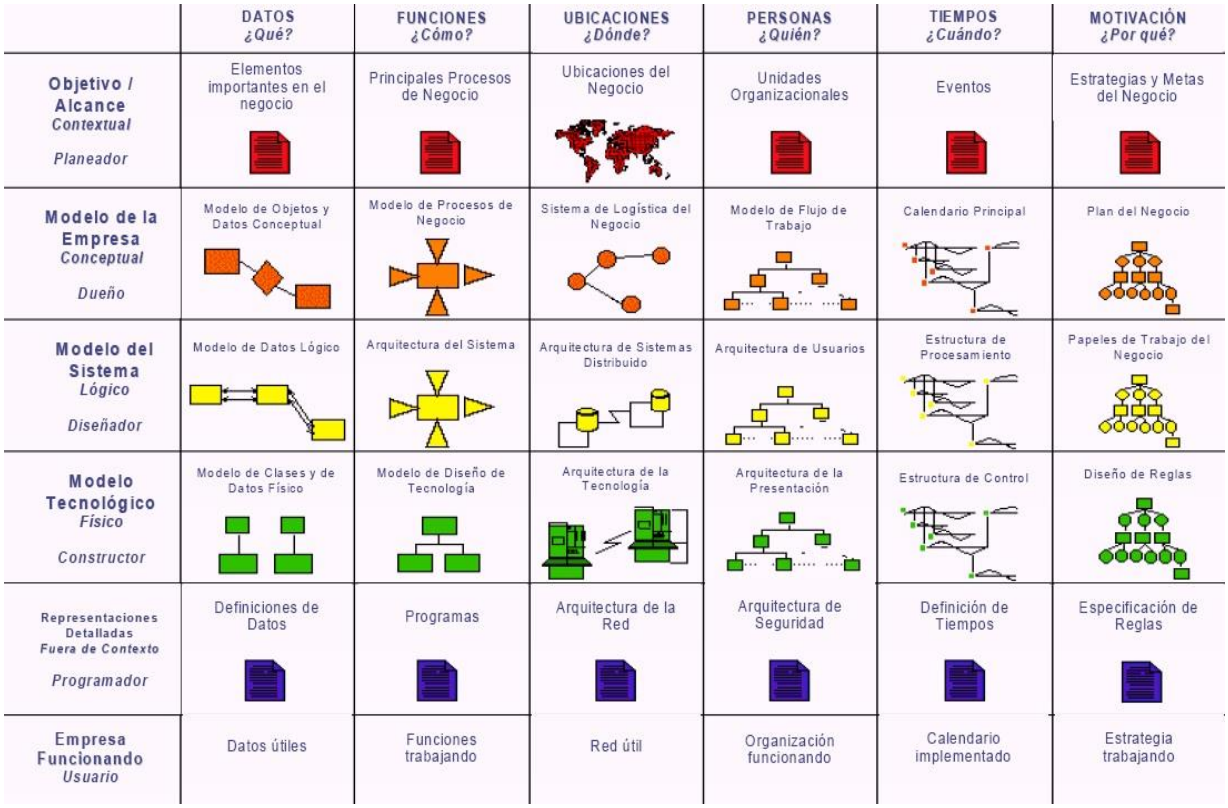


Figura 3. Componentes AE – Matriz de Jhon Zachman

Fuente: https://www.emaze.com/@ACLTITIZ/Arquitectura-tiEn

John A. Zachman, creador del Framework, define al mismo como un proyecto, que nace de la intersección de dos clasificaciones que históricamente se han utilizado por miles de años. Siendo la primera de éstas clasificaciones las preguntas consideradas como primitivas dentro de la comunicación: ¿Qué?, ¿Cómo?, ¿Cuándo?, ¿Quién?, ¿Dónde? y ¿Por qué? Puesto a que las respuestas a estas interrogantes facilita la elaboración de una descripción completa y comprensible de ideas complejas. La segunda de estas clasificaciones es derivada de la transformación de una idea abstracta en una instanciación, mediante una serie de pasos marcados como: Identificación, Definición, Representación, Especificación, Configuración e Instalación.

La razón del empleo de esta forma de clasificación fue que ambas clasificaciones se utilizan de una manera empírica para las representaciones descriptivas (arquitecturas) de edificios, aviones u otros productos comerciales de gran complejidad; de tal forma se asegura que este Framework es la estructura fundamental de una Arquitectura Empresarial, ya que contiene un set de representaciones relevantes para la descripción de una Arquitectura.

De una forma específica podemos decir que este Framework es una ontología, una teoría que establece la existencia de un conjunto estructurado de componentes esenciales para un objeto en el cual las expresiones explícitas de éstas son básicas e incluso obligatorias para la creación, operación y cambios de los mismos.

Zachman no es una metodología para la creación de la implementación (o instanciación) del objeto en cuestión sino la ontología para la descripción del objeto; por el contrario, una metodología es una descripción para la elaboración de un proceso.

El Framework de Zachman describe un modelo integral de la infraestructura de la información de la empresa desde seis perspectivas: planificador, propietario, diseñador, constructor, subcontratistas, y el sistema de trabajo. No hay ninguna orientación sobre la secuencia, proceso o aplicación del marco. La atención se centra en garantizar que todos los aspectos de una empresa están bien organizados y muestra relaciones claras que garanticen un sistema completo, independientemente del orden en el que están establecidos.[8]

4.4 Arquitectura Empresarial en el contexto de MINTIC – Colombia

Es una práctica estratégica que consiste en analizar integralmente a las entidades o instituciones desde diferentes perspectivas o dimensiones, con el propósito de obtener su estado actual y la visión a largo plazo, permitiendo alinear la estrategia, los procesos, los datos, aplicaciones e infraestructura tecnológica, con el fin de agregar valor a las organizaciones. En general, dentro de la Arquitectura Empresarial se identifican cuatro componentes, pero para el caso colombiano son seis: Estrategia, Gobierno de TI, Información, Sistemas de Información, Servicios de Tecnología y Uso y Apropiación. Su principal objetivo es garantizar la correcta alineación de la tecnología y los procesos de negocio en una organización, con el propósito de alcanzar el cumplimiento de sus objetivos estratégicos.

El objetivo es generar valor a través de las Tecnologías de la Información para que se ayude a materializar la visión de la entidad. Cuando se desarrolla en conjunto para grupos de instituciones públicas, permite además asegurar una coherencia global, que resulta estratégica para promover el desarrollo del país. Una arquitectura se descompone en varias estructuras o dimensiones para facilitar su estudio. En el caso colombiano, se plantea la realización de la arquitectura misional o de negocio y la definición de la arquitectura de TI, cuya descomposición se hizo en seis dominios: Estrategia de TI, Gobierno de TI, Información, Sistemas de Información, Servicios Tecnológicos y Uso y Apropiación.

Se dice que una institución cuenta con una Arquitectura Empresarial cuando ha desarrollado un conjunto de ejercicios o proyectos, siguiendo la práctica estratégica antes mencionada; además que ha logrado diseñar un mapa de ruta de transformación de TI y lo ha integrado al Plan Estratégico de Tecnologías de Información (PETI). Los artefactos creados durante un ejercicio o proyecto de arquitectura empresarial se almacenan en un repositorio e incluyen, entre otros, una descripción detallada de la arquitectura empresarial actual, de la arquitectura

empresarial objetivo, un análisis de brecha y un mapa de ruta para lograr llegar a la meta o punto ideal.[9].

Por otra parte la **Arquitectura Empresarial de TI** es un componente de la arquitectura empresarial en el que se definen vistas lógicas de información, sistemas de información, infraestructura, servicios tecnológicos y un ambiente de gestión de TI para contribuir con la transformación empresarial.

El 6 de noviembre de 2014, el ministerio de las tecnologías y las comunicaciones realizó oficialmente el lanzamiento del marco de referencia para la arquitectura de TI del Estado colombiano y la cual obliga a todas los entes públicos a dar cumplimiento a través del decreto 2693 de 2012, por medio del cual se establecen los lineamentos generales de la Estrategia de Gobierno en Línea de la República de Colombia y se reglamentan parcialmente las Leyes 1341 de 2009, 1450 de 2011, y se dictan otras disposiciones.

El Marco de Referencia de Arquitectura Empresarial, en adelante Marco de Referencia de AE, es un modelo de referencia puesto a disposición de las entidades del Estado colombiano, para ser utilizado como soporte de la estructuración de las arquitecturas empresariales, tanto sectoriales como institucionales, y que se adaptará a las necesidades y características propias de cada sector y entidad respectivamente. El marco establece los elementos que, de manera común, deben considerarse para la implementación de AE en el Estado.
La estructura del Marco de Referencia de AE para el Estado Colombiano está compuesta por los siguientes elementos:

a) Principios

b) Dominios

c) Base de Conocimiento

a) **Principios:** El Marco de Referencia de Arquitectura Empresarial para la gestión de Tecnologías de la Información del Estado colombiano, se desarrollará con fundamento en los principios consagrados en los Artículos 209 de la Constitución Política, 3° de la Ley 489 de 1998 y 3° de la Ley 1437 de 2011 y, adicionalmente, en los siguientes:

Excelencia al servicio al ciudadano: Propender por el fin superior de fortalecer la relación de los ciudadanos con el Estado.

Inversión con buena relación costo/beneficio: Propender porque las inversiones de TI representen un retorno medido, por el impacto de los proyectos.

Racionalización: Buscar la optimización en el uso de los recursos teniendo en cuenta criterios de pertinencia y reutilización.

Estandarización: Ser la base para la definición de los lineamientos, políticas y procedimientos que faciliten la evolución de la gestión de TI del Estado colombiano hacía un modelo estandarizado.

Interoperabilidad: Fortalecer los esquemas de interoperabilidad que estandaricen y faciliten el intercambio de información entre entidades y sectores, manejo de fuentes únicas de información y la habilitación de servicios.

Viabilidad en el mercado: Ofrecer definiciones que motiven al mercado a plantear y diseñar soluciones según las necesidades del Estado colombiano.

Federación: El Marco de Referencia de Arquitectura Empresarial

Co-creación: Permitir componer nuevas soluciones y servicios sobre lo ya construido y definido con la participación de los todas aquellas personas u organizaciones que influyen o son afectadas por el Marco de Referencia.

Escalabilidad: Permitir la evolución continua y la adición de todos los componentes y dominios que lo componen, sin perder calidad ni articulación.

Seguridad de la Información: Permitir la definición, implementación y verificación de controles de seguridad de la información.

Sostenibilidad: Aportar al equilibrio ecológico por medio de las TI.

Neutralidad Tecnológica: Se tendrá la definición del Decreto 2693 de 2012, "por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en Línea de la República de Colombia…", el cual dice: "El Estado garantizará la libre adopción de tecnologías, teniendo en cuenta recomendaciones, conceptos y normativas de los organismos internacionales competentes e idóneos en la materia, que permitan fomentar la eficiente prestación de servicios, contenidos y aplicaciones que usen Tecnologías de la Información y las Comunicaciones, y garantizar la libre y leal competencia y que su adopción sea armónica con el desarrollo ambiental sostenible".[10]

b) Dominios o dimensiones: El Marco de Referencia de AE para el Estado colombiano incorpora los siguientes seis dominios:

1- **Dominio de Información**: define estándares y lineamientos para la gestión de información como principal generador de valor estratégico para la institución. Comprende la definición de los siguientes aspectos: diseño de los servicios de información, la gestión de la calidad de la misma, la gestión del ciclo de vida del dato y de información, el análisis de información y el desarrollo de capacidades para el uso estratégico de ésta.

2- **Dominio de Sistemas de Información**: define estándares y lineamientos para la gestión de los sistemas de información, incluyendo su arquitectura, ciclo de vida, las aplicaciones que los conforman y los procesos de implementación y soporte.

3- **Dominio de Servicios Tecnológicos**: define estándares y lineamientos para la gestión de la infraestructura tecnológica que soporta los sistemas y los servicios de información, así como los servicios requeridos para su operación. Comprende la definición de la infraestructura tecnológica, la gestión de la capacidad de los servicios de TI, la gestión de la operación y la gestión de los servicios de soporte.

4- **Dominio de Estrategia de TI:** define estándares y lineamientos, para diseñar la estrategia de TI y lograr su alineación con las estrategias del Estado y **el sector a la que pertenece.**

5- **Dominio de Gobierno de TI:** define estándares y lineamientos para diseñar e implementar esquemas de gobernabilidad de TI, **alinear los procesos de la entidad con los del sector** e incorporar políticas de TI en las entidades y procesos para la gestión de TI, gestión por procesos de TI, estructura organizacional de TI, gestión de proveedores y gestión de proyectos.

6- **Dominio de Uso y Apropiación:** define estándares y lineamientos para el Uso y Apropiación de TI, el cual incluye la gestión del cambio y gestión de grupos de interés.

c) Base de conocimiento*:* provee un portafolio de instrumentos y herramientas que guían y ayudan a la implementación del Marco de Referencia de AE e incluye entre otros: estándares, lineamientos, guías, modelo de gestión de TI, mejores prácticas, soluciones y casos de éxito.

Lineamientos: Son una orientación de carácter general, corresponden a una disposición o directriz que deben ser implementadas en las entidades del Estado colombiano.

Estándares: especificaciones técnicas que tienen una función instrumental y que responden a cómo se implementa un lineamiento o elemento. Existen estándares de industria o estándares generales.

Guías: definición procedimental que detalla por medio de actividades los pasos que debe ejecutar una entidad para producir un resultado. Provee las instrucciones de cómo adoptar el estándar. Una guía puede ser un instructivo, procedimiento, lista de verificación, una formulación, modelo matemático o manual. Existen Guías referenciadas y Guías desarrolladas.

Mejores prácticas: identifica y relaciona la mejor práctica aplicable para apoyar o implementar en el dominio.

Soluciones: identifica y relaciona las herramientas o sistemas de información existentes en el Estado colombiano que apoyan el dominio.

Indicadores del ámbito: define cómo se mide la ejecución del ámbito. Los indicadores son obligatorios en el dominio.

Normatividad: relaciona la normatividad del entorno regulatorio colombiano que aplica al dominio. La normatividad es opcional.

Mejores prácticas: relaciona las mejores prácticas internacionales que aplican al dominio. Son opcionales.

Modelo de organización: Descripción de las funciones necesarias para estructurar el dominio en las entidades. El Modelo organizacional es obligatorio en el dominio.

Modelo de gestión de Tecnologías de la Información: esta herramienta facilita la aplicación práctica del Marco de Referencia de AE. El modelo de gestión de TI adapta la tecnología y la pone al alcance de la mano de todos los usuarios de las entidades públicas. Además contribuye al mejoramiento de la gestión organizacional porque facilita la administración y el control de los recursos de TI para brindar información oportuna y objetiva para la toma de decisiones en todos los niveles de las instituciones del Estado. Cuenta con instrumentos prácticos tales como: procesos, procedimientos, métodos, funciones, mecanismos de control y adopción de buenas prácticas de gestión de tecnología. [10]

4.4.1 Capas del Modelo de Arquitectura Empresarial en el contexto de MINTIC – Colombia.

Por estructura y navegabilidad del Marco de Referencia se plantearon cuatro capas:

Capa 1 Dominios, **capa 2 Ámbitos, capa 3 Lineamientos** y **capa 4 Instrumentos.**

A continuación se pueden visualizar las cuatro capas que componen el Marco de Referencia de AE:

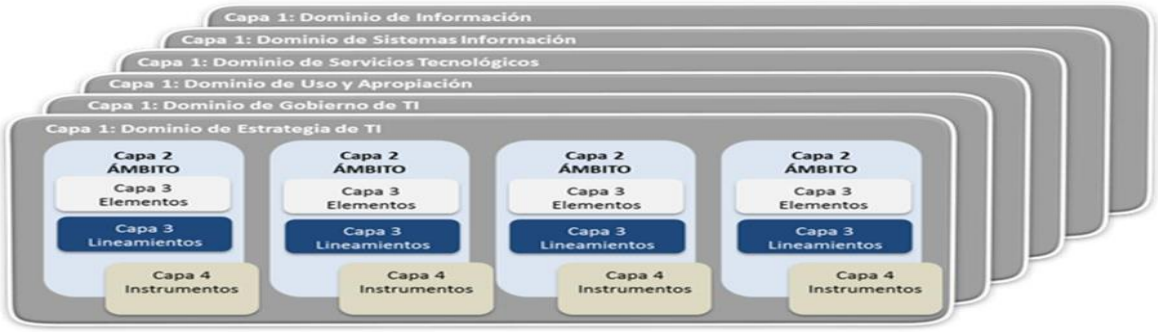


Figura 4. Capas AE – MINTIC- Colombia
Fuente: http://www.mintic.gov.co/gestionti/615/articles-4211_sumen_del_diseno_y_especificacion_del_Marco_de_Referencia_de_la_Arquitectura_Empresarial_para_la_Gestion_TI_del_Estado.pdf

Capa 1: el escenario objetivo de este Marco de Referencia de AE está compuesto por una primera capa de seis, y son los dominios.

Capa 2: la siguiente capa de abstracción se denomina **Ámbito**, la cual representa áreas o temáticas que aborda el dominio.

Capa 3: en la tercera capa se encuentran **los Elementos y Lineamientos a nivel de Ámbito**, en cuyo caso, los primeros representan temas de relevancia de un ámbito que se pretende profundizar y los segundos representan el *qué* se espera que suceda.

Capa 4: por último se cuenta con una cuarta capa que representa la **base de conocimiento del Marco de Referencia de AE.** Esta capa provee un portafolio de instrumentos del Marco de Referencia de AE.

4.4.2 Componentes de la Arquitectura Empresarial en el contexto de MINTIC – Colombia.

Figura 5. Componentes AE – MINTIC- Colombia

Fuente: http://www.mintic.gov.co/gestionti/615/articles-4211_sumen_del_diseno_y_especificacion_del_Marco_de_Referencia_de_la_Arquitectura_Empresarial_para_la_Gestion_TI_del_Estado.pdf

Los dominios del Marco de Referencia de AE, para el Estado colombiano están alineados con las definiciones hechas en el Diseño Contextual del Marco de Referencia de AE [3] y son similares a los niveles que se presentan en los conceptos tradicionales de Arquitectura Empresarial, como se puede ver a continuación:

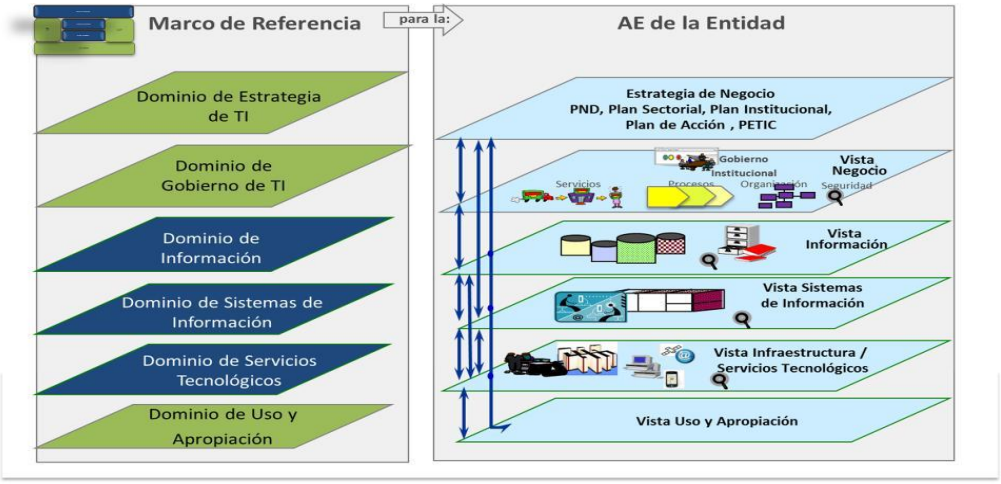


Figura 6. Dominios AE – MINTIC- Colombia – Detallados

Fuente: http://www.mintic.gov.co/gestionti/615/articles-4211_sumen_del_diseno_y_especificacion_del_Marco_de_Referencia_de_la_Arquitectura_Empresarial_para_la_Gestion_TI_del_Estado.pdf

El dominio de Estrategia de TI:

Figura 7. Dominios Estrategia de TI– MINTIC- Colombia – Detallados

Fuente: http://www.mintic.gov.co/gestionti/615/articles-4211_sumen_del_diseno_y_especificacion_del_Marco_de_Referencia_de_la_Arquitectura_Empresarial_para_la_Gestion_TI_del_Estado.pdf

El dominio de Gobierno de TI:

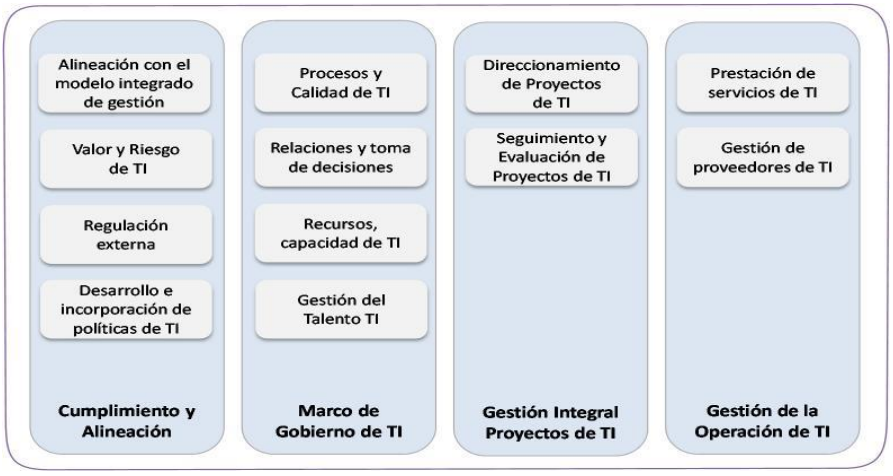


Figura 8. Dominio Gobierno de TI– MINTIC- Colombia – Detallados

Fuente: http://www.mintic.gov.co/gestionti/615/articles-4211_sumen_del_diseno_y_especificacion_del_Marco_de_Referencia_de_la_Arquitectura_Empresarial_para_la_Gestion_TI_del_Estado.pdf

El dominio de Información:

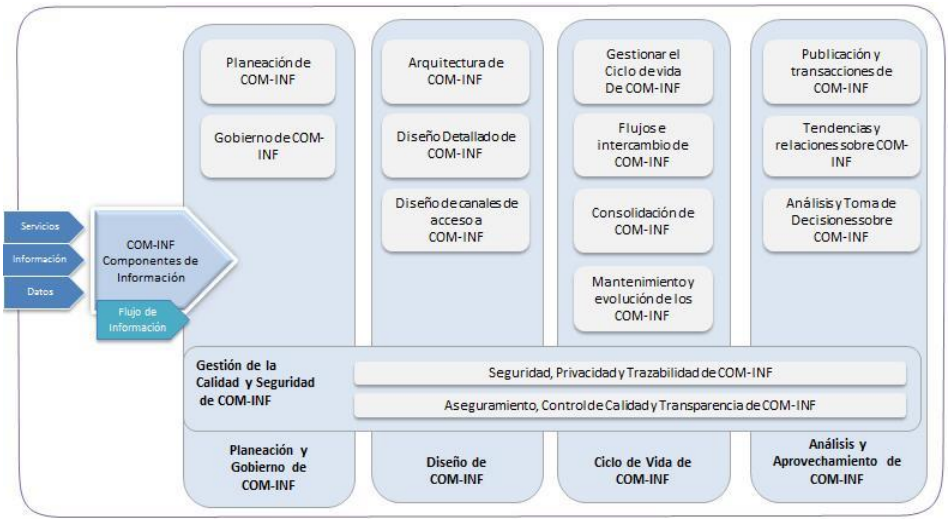


Figura 9. Dominio de Información– MINTIC- Colombia – Detallados

Fuente: http://www.mintic.gov.co/gestionti/615/articles-4211_sumen_del_diseno_y_especificacion_del_Marco_de_Referencia_de_la_Arquitectura_Empresarial_para_la_Gestion_TI_del_Estado.pdf

El dominio de Sistemas de Información:

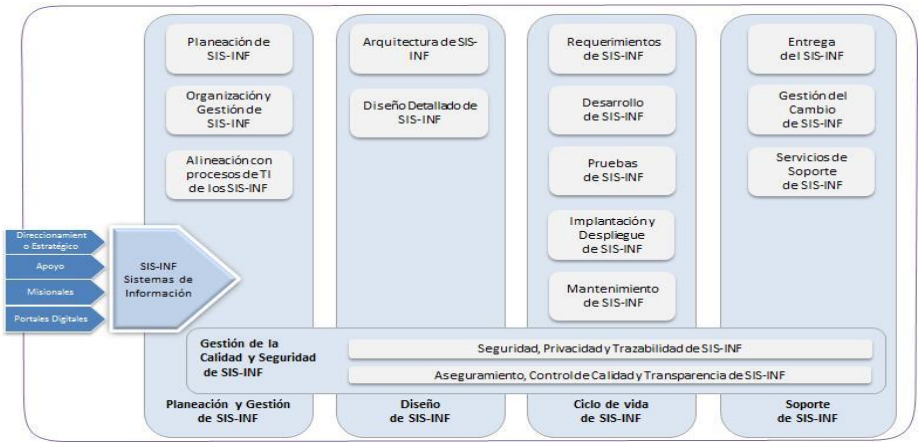


Figura 10. Dominio de Sistemas de Información– MINTIC- Colombia – Detallados

Fuente: http://www.mintic.gov.co/gestionti/615/articles-4211_sumen_del_diseno_y_especificacion_del_Marco_de_Referencia_de_la_Arquitectura_Empresarial_para_la_Gestion_TI_del_Estado.pdf

El dominio de servicios tecnológicos:

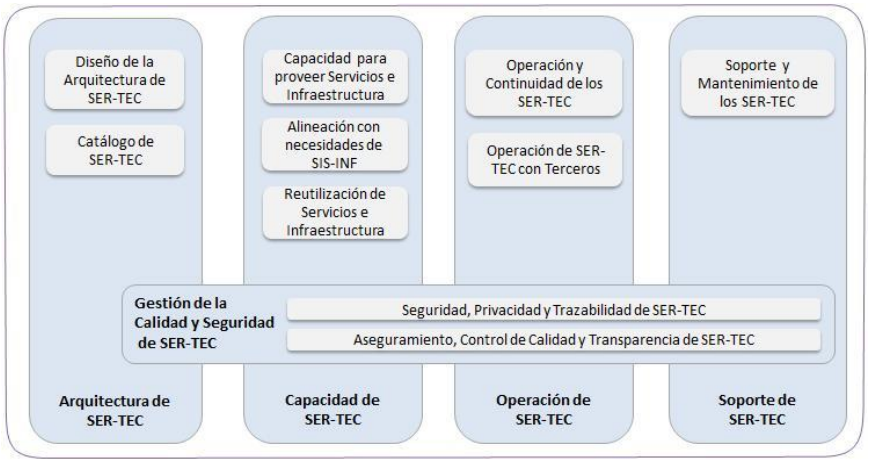


Figura 11. Dominio de servicios tecnológicos – MINTIC- Colombia – Detallados

Fuente: http://www.mintic.gov.co/gestionti/615/articles-4211_sumen_del_diseno_y_especificacion_del_Marco_de_Referencia_de_la_Arquitectura_Empresarial_para_la_Gestion_TI_del_Estado.pdf

El dominio de uso y apropiación:

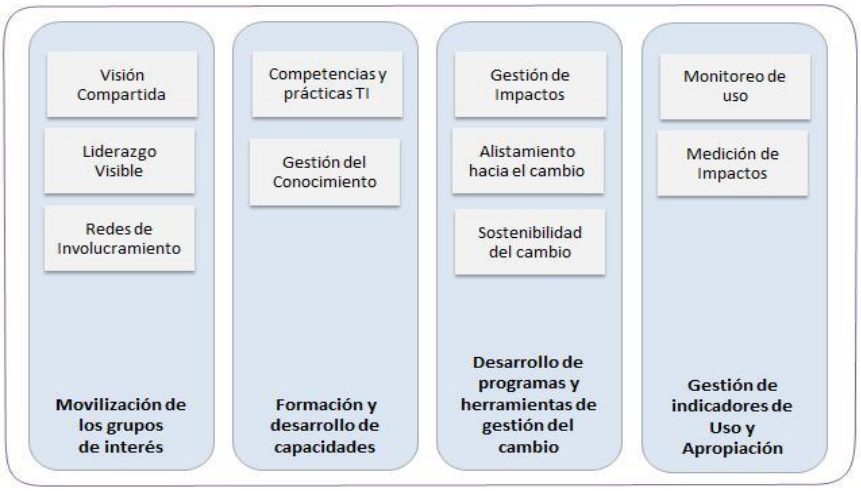


Figura 12. Dominio de uso y apropiación – MINTIC- Colombia – Detallados

Fuente: http://www.mintic.gov.co/gestionti/615/articles-4211_sumen_del_diseno_y_especificacion_del_Marco_de_Referencia_de_la_Arquitectura_Empresarial_para_la_Gestion_TI_del_Estado.pdf

4.5. F.G.N – Fiscalía General de la Nación (Dirección de Control Interno – Subdirección de las TICs)

La Fiscalía General nació en 1991 con la promulgación de la nueva Constitución Política y empezó a operar el 1 de julio de 1992.

Es una entidad de la rama judicial del poder público con plena autonomía administrativa y presupuestal, cuya función está orientada a brindar a los ciudadanos una cumplida y eficaz administración de justicia.[11]

De acuerdo con el **Artículo 249** de la constitución política de Colombia, la Fiscalía General de la Nación estará integrada por el Fiscal General, los fiscales delegados y los demás funcionarios que determine la ley. El Fiscal General de la Nación será elegido para un período de cuatro años por la Corte Suprema de Justicia, de terna enviada por el Presidente de la República y no podrá ser reelegido. Debe reunir las mismas calidades exigidas para ser Magistrado de la Corte Suprema de Justicia. La Fiscalía General de la Nación forma parte de la rama judicial y tendrá autonomía administrativa y presupuestal.

Artículo 250. Corresponde a la Fiscalía General de la Nación, de oficio o mediante denuncia o querella, investigar los delitos y acusar a los presuntos infractores ante los juzgados y tribunales competentes. Se exceptúan los delitos cometidos por miembros de la Fuerza Pública en servicio activo y en relación con el mismo servicio. Para tal efecto la Fiscalía General de la Nación deberá: 1. Asegurar la comparecencia de los presuntos infractores de la ley penal, adoptando las medidas de aseguramiento. Además, y si fuere del caso, tomar las medidas necesarias para

hacer efectivos el restablecimiento del derecho y la indemnización de los perjuicios ocasionados por el delito. 2. Calificar y declarar precluidas las investigaciones realizadas. 3. Dirigir y coordinar las funciones de policía judicial que en forma permanente cumplen la Policía Nacional y los demás organismos que señale la ley. 4. Velar por la protección de las víctimas, testigos e intervinientes en el proceso. 5. Cumplir las demás funciones que establezca la ley. El Fiscal General de la Nación y sus delegados tienen competencia en todo el territorio nacional. La Fiscalía General de la Nación está obligada a investigar tanto lo favorable como lo desfavorable al imputado, y a respetar sus derechos fundamentales y las garantías procesales que le asisten.

Artículo 251. Son funciones especiales del Fiscal General de la Nación: 1. Investigar y acusar, si hubiere lugar, a los altos funcionarios que gocen de fuero constitucional, con las excepciones previstas en la Constitución. 2. Nombrar y remover, de conformidad con la ley, a los empleados bajo su dependencia. 3. Participar en el diseño de la política del Estado en materia criminal y presentar proyectos de ley al respecto. 4. Otorgar atribuciones transitorias a entes públicos que puedan cumplir funciones de policía judicial, bajo la responsabilidad y dependencia funcional de la Fiscalía General de la Nación. 5. Suministrar al Gobierno información sobre las investigaciones que se estén adelantando, cuando sea necesaria para la preservación del orden público.

Artículo 252. Aun durante los Estados de Excepción de que trata la Constitución en sus artículos 212 y 213, el Gobierno no podrá suprimir, ni modificar los organismos ni las funciones básicas de acusación y juzgamiento.

Artículo 253. La ley determinará lo relativo a la estructura y funcionamiento de la Fiscalía General de la Nación, al ingreso por carrera y al retiro del servicio, a las inhabilidades e incompatibilidades, denominación, calidades, remuneración,

prestaciones sociales y régimen disciplinario de los funcionarios y empleados de su dependencia.[12]

4.5.1 Misión de la Fiscalía General de la Nación

La Fiscalía General de la Nación ejerce la acción penal y participa en el diseño de la política criminal del Estado; garantiza la tutela judicial efectiva de los derechos de los intervinientes en el proceso penal; genera confianza y seguridad jurídica en la sociedad mediante la búsqueda de la verdad, la justicia y la reparación.[13]

4.5.2 Visión de la Fiscalía General de la Nación

En el 2016, la Fiscalía General de la Nación contará con un sistema de investigación integral y será reconocida por el diseño y ejecución de políticas públicas vanguardistas que le permitirán enfrentar con éxito las diversas formas de criminalidad. Su tarea se verá apoyada en la profesionalización del talento humano y el desarrollo y aplicación de herramientas innovadoras de tecnología y comunicación, que garanticen la independencia, la autonomía, el acceso a la justicia y la efectividad de la acción penal.

4.5.3 Estructura Orgánica de la Fiscalía General de la Nación

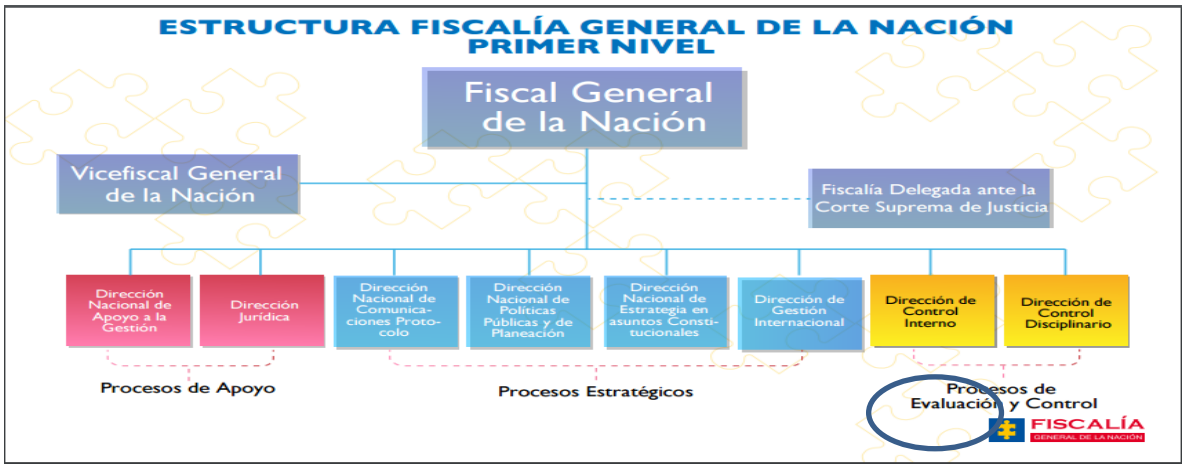


Figura 13. Organigrama FGN – Primer Nivel

Fuente: http://www.fiscalia.gov.co/colombia/wp-content/uploads/ORG1.pdf

Figura 14. Organigrama FGN – Segundo Nivel

Fuente: http://www.fiscalia.gov.co/colombia/wp-content/uploads/ORG2.pdf

Figura 15. Organigrama FGN – Tercer Nivel

Fuente: http://www.fiscalia.gov.co/colombia/wp-content/uploads/ORG3.pdf

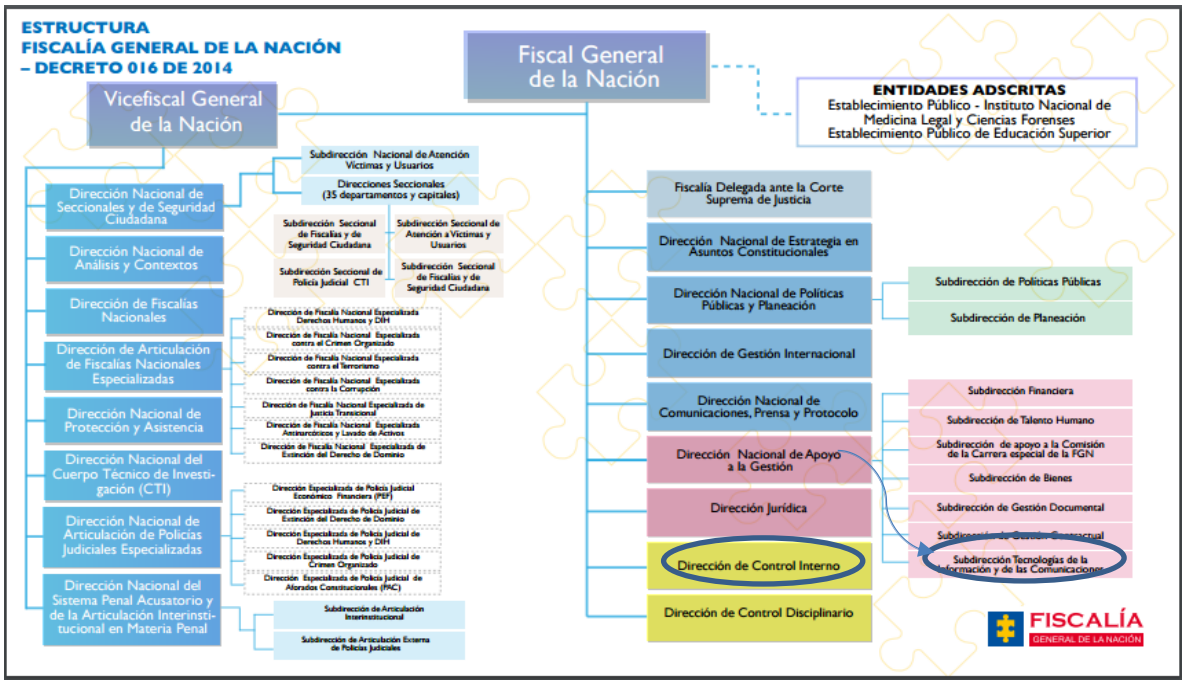


Figura 16. Organigrama FGN – Decreto 016 de 2014

Fuente: http://www.fiscalia.gov.co/colombia/wp-content/uploads/ORG4.pdf

Figura 17. Mapa de proceso institucional - FGN – Decreto 016 de 2014

Fuente: http://www.fiscalia.gov.co/colombia/wp-content/uploads/mapa-de-procesos.pdf

4.5.4 Funciones de la Dirección de Control Interno contenidas en la Ley 87 de 1993:

a) Planear, dirigir y organizar la verificación y evaluación del sistema de control Interno;

b) Verificar que el Sistema de Control Interno esté formalmente establecido dentro de la organización y que su ejercicio sea intrínseco al desarrollo de las funciones de todos los cargos y, en particular, de aquellos que tengan responsabilidad de mando;

c) Verificar que los controles definidos para los procesos y actividades de la organización, se cumplan por los responsables de su ejecución y en especial, que las áreas o empleados encargados de la aplicación del régimen disciplinario ejerzan adecuadamente esta función;

d) Verificar que los controles asociados con todas y cada una de las actividades de la organización estén adecuadamente definidos, sean apropiados y se mejoren permanentemente, de acuerdo con la evolución de la entidad;

e) Velar por el cumplimiento de las leyes, normas, políticas, procedimientos, planes, programas, proyectos y metas de la organización y recomendar los ajustes necesarios;

f) Servir de apoyo a los directivos en el proceso de toma de decisiones, a fin que se obtengan los resultados esperados;

g) Verificar los procesos relacionados con el manejo de los recursos, bienes y los sistemas de información de la entidad y recomendar los correctivos que sean necesarios;

h) Fomentar en toda la organización la formación de una cultura de control que contribuya al mejoramiento continuo en el cumplimiento de la misión institucional;

i) Evaluar y verificar la aplicación de los mecanismos de participación ciudadana, que en desarrollo del mandato constitucional y legal, diseñe la entidad correspondiente;

j) Mantener permanentemente informados a los directivos acerca del estado del control interno dentro de la entidad, dando cuenta de las debilidades detectadas y de las fallas en su cumplimiento;

k) Verificar que se implanten las medidas respectivas recomendadas;

l) Las demás que le asigne el jefe del organismo o entidad, de acuerdo con el carácter de sus funciones.

PARÁGRAFO. En ningún caso, podrá el asesor, coordinador, auditor interno o quien haga sus veces, participar en los procedimientos administrativos de la entidad a través de autorizaciones o refrendaciones.[15]

4.5.5 Funciones de la Dirección de Control Interno contenidas en el Decreto 016 de 2014

1. Planear, dirigir y organizar la verificación y evaluación del Sistema de Control Interno de la Fiscalía General de la Nación.

2. Verificar que el Sistema de Control Interno esté formalmente establecido dentro de la entidad y que su ejercicio sea intrínseco al desarrollo de las funciones de todos los cargos y en particular, de aquellos que tengan responsabilidad de mando.

3. Verificar que los controles definidos para los procesos y actividades de la Fiscalía General de la Nación se cumplan por los responsables de su ejecución.

4. Verificar que los controles asociados con todas y cada una de las actividades de la Fiscalía General de la Nación, estén adecuadamente definidos, sean apropiados y se mejoren permanentemente.

5. Velar por el cumplimiento de las leyes, normas, políticas, procedimientos, planes, programas, proyectos y metas de la Fiscalía General de la Nación y recomendar los ajustes necesarios.

6. Asesorar en la elaboración de la metodología para la identificación del riesgo y hacer seguimiento a las acciones para la mitigación de los mismos.

7. Proponer políticas o estrategias para la administración del riesgo que permitan desarrollar o fijar acciones efectivas de control.

8. Evaluar la existencia y efectividad de los controles establecidos por los líderes de los procesos para el desarrollo de sus funciones y competencias.

9. Fomentar la cultura del autocontrol que contribuya al mejoramiento continuo en el cumplimiento de la misión institucional.

10. Evaluar y verificar la aplicación de los mecanismos de participación ciudadana, que en desarrollo del mandato Constitucional y legal, diseñe la Fiscalía General de la Nación.

11. Realizar el seguimiento y evaluación a la gestión y resultados de las dependencias de la Fiscalía General de la Nación, presentar los informes, recomendar las acciones de mejora a que haya lugar y verificar su cumplimiento.

12. Publicar un informe pormenorizado del estado del control interno de la Fiscalía General de la Nación, en la página web, de acuerdo con la Ley 1474 de 2011 y en las normas que la modifiquen o adicionen.

13. Hacer seguimiento a las dependencias encargadas de atender a las víctimas y usuarios y rendir al Fiscal General de la Nación un informe semestral.

14. Asesorar al Fiscal General de la Nación en las relaciones institucionales y funcionales con los organismos de control.

15. Impartir los lineamientos y directrices para el cumplimiento de las funciones de control interno en las Direcciones Seccionales.

16. Elaborar e implementar los planes operativos anuales en el ámbito de su competencia, de acuerdo con la metodología diseñada por la Subdirección de Planeación.

17. Aplicar las directrices y lineamientos del Sistema de Gestión Integral de la Fiscalía General de la Nación.

18. Las demás que le sean asignadas por la ley o delegadas por el Fiscal General de la Nación [15].

4.5.6 Sistema de Evaluación y Seguimiento Integral en la F.G.N

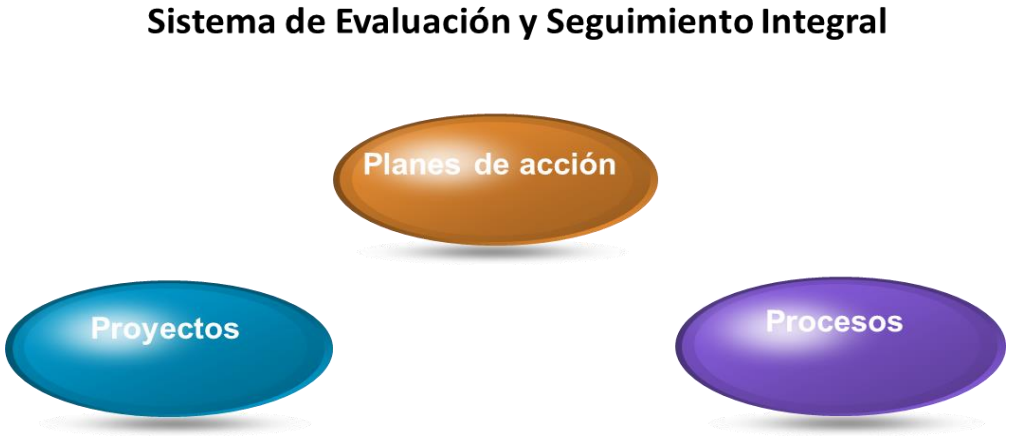


Figura 18 Sistema Evaluación Seguimiento Integral FGN

Fuente. Sistema de Gestión Integral FGN

4.5.7 Funciones de la Subdirección Tecnologías de la información y las Comunicaciones

1. Asesorar al Fiscal General de la Nación en la definición de las políticas, planes, programas y procedimientos relacionados con el uso de las tecnologías de información y comunicaciones, que contribuyan a incrementar la eficiencia y eficacia en las diferentes dependencias de la Entidad, así como garantizar la calidad en la prestación de los servicios.
2. Liderar, coordinar y monitorear la plataforma de tecnologías de la información y la comunicación de la Fiscalía General de ja Nación, que apoye el cumplimiento de sus funciones.

3. Liderar, coordinar y articular los diferentes sistemas de información de la entidad. Para tal efecto, adelantará y presidirá comités técnicos con los respectivos coordinadores de los sistemas de información de las diferentes dependencias de la Fiscalía.
4. Elaborar y hacer seguimiento al Plan Maestro de las Tecnologías de la Información y las Comunicaciones.
5. Promover e intervenir en las actividades y programas que tiendan a incorporar el uso de las tecnologías de la información y las comunicaciones en el desarrollo de las actividades de la Fiscalía General de la Nación.
6. Diseñar, implementar e integrar soluciones informáticas, basadas en gestión de procesos, que de soporte a todas las áreas misionales de la Fiscalía General de la Nación.
7. Definir las necesidades que en materia de sistemas de información requiera la Fiscalía General de la Nación, para el desarrollo de sus funciones y coordinar su adquisición con la Dirección de Apoyo a la Gestión.
8. Consolidar, desarrollar e implementar las diferentes estrategias, estándares de datos e integración de procesos y líneas de políticas gubernamentales sobre el uso y alcance de las tecnologías de la información y las comunicaciones.
9. Gestionar, atender, proponer e implementar las políticas y acciones relativas a la seguridad y oficialidad de la información y de la plataforma tecnológica de la Fiscalía General de la Nación.
10. Asesorar a las Direcciones Seccionales en el ámbito de su competencia.
11. Elaborar e implementar los planes operativos anuales en el ámbito de su competencia, de acuerdo con la metodología diseñada por la Subdirección de Planeación.

12. Aplicar las directrices y lineamientos del Sistema de Gestión Integral de la Fiscalía General de la Nación.
13. Las demás que le sean asignadas por la ley o delegadas por el Fiscal General de la Nación o por el Director de Apoyo a la Gestión de la Fiscalía General de la Nación.[16]

4.5.8 Funciones de la Subdirección Tecnologías de la información y las Comunicaciones contenidas en el Decreto 016 de 2014 artículo 39.

La Subdirección de Tecnologías de la Información y las Comunicaciones cumplirá las siguientes funciones:

1. Asesorar al Fiscal General de la Nación en la definición de las políticas, planes, programas y procedimientos relacionados con el uso de las tecnologías de información y comunicaciones, que contribuyan a incrementar la eficiencia y eficacia en las diferentes dependencias de la Entidad, así como garantizar la calidad en la prestación de los servicios.

2. Liderar, coordinar y monitorear la plataforma de tecnologías de la información y la comunicación de la Fiscalía General de la Nación, que apoye el cumplimiento de sus funciones.

3. Liderar, coordinar y articular los diferentes sistemas de información de la entidad. Para tal efecto, adelantará y presidirá comités técnicos con los respectivos coordinadores de los sistemas de información de las diferentes dependencias de la Fiscalía.

4. Elaborar y hacer seguimiento al Plan Maestro de las Tecnologías de la Información y las Comunicaciones.

5. Promover e intervenir en las actividades y programas que tiendan a incorporar el uso de las tecnologías de la información y las comunicaciones en el desarrollo de las actividades de la Fiscalía General de la Nación.

6. Diseñar, implementar e integrar soluciones informáticas, basadas en gestión de procesos, que de soporte a todas las áreas misionales de la Fiscalía General de la Nación.

7. Definir las necesidades que en materia de sistemas de información requiera la Fiscalía General de la Nación, para el desarrollo de sus funciones y coordinar su adquisición con la Dirección de Apoyo a la Gestión. DECRETO NUMERO 016 HOJA 37 Continuación del decreto "Por el cual se modifica y define la estructura orgánica y funcional de la Fiscalía General de la Nación".

8. Consolidar, desarrollar e implementar las diferentes estrategias, estándares de datos e integración de procesos y líneas de políticas gubernamentales sobre el uso y alcance de las tecnologías de la información y las comunicaciones.

9. Gestionar, atender, proponer e implementar las políticas y acciones relativas a la seguridad y oficialidad de la información y de la plataforma tecnológica de la Fiscalía General de la Nación.

10. Asesorar a las Direcciones Seccionales en el ámbito de su competencia.

11. Elaborar e implementar los planes operativos anuales en el ámbito de su competencia, de acuerdo con la metodología diseñada por la Subdirección de Planeación.

12. Aplicar las directrices y lineamientos del Sistema de Gestión Integral de la Fiscalía General de la Nación.

13. Las demás que le sean asignadas por la ley o delegadas por el Fiscal General de la Nación o por el Director de Apoyo a la Gestión de la Fiscalía General de la Nación. [16]

4.6. COBIT

4.6.1 Marco COBIT

Objetivos de Control para Información y Tecnologías Relacionadas (COBIT, en inglés: Control Objectives for Information and related Technology) es una guía de mejores prácticas presentado como framework, dirigida al control y supervisión de tecnología de la información (TI). Mantenido por ISACA (en inglés: Information Systems Audit and Control Association) y el IT GI (en inglés: IT Governance Institute), tiene una serie de recursos que pueden servir de modelo de referencia para la gestión de TI, incluyendo un resumen ejecutivo, un framework, objetivos de control, mapas de auditoría, herramientas para su implementación y principalmente, una guía de técnicas de gestión.

COBIT es un marco de gobierno de las tecnologías de información que proporciona una serie de herramientas para que la gerencia pueda conectar los requerimientos de control con los aspectos técnicos y los riesgos del negocio. COBIT permite el desarrollo de las políticas y buenas prácticas para el control de las tecnologías en toda la organización. COBIT enfatiza el cumplimiento regulatorio, ayuda a las organizaciones a incrementar su valor a través de las tecnologías, y permite su alineamiento con los objetivos del negocio.

4.6.2 COBIT 5.0

Isaca lanzó el 10 de abril del 2012 la nueva edición de este marco de referencia. COBIT 5 es la última edición del framework mundialmente aceptado, el cual

proporciona una visión empresarial del Gobierno de TI que tiene a la tecnología y a la información como protagonistas en la creación de valor para las empresas.

COBIT 5 se basa en COBIT 4.1, y a su vez lo amplía mediante la integración de otros importantes marcos y normas como ValIT y RiskIT, Information Technology Infrastructure Library (ITIL ®) y las normas ISO relacionadas en esta norma.

COBIT 5 ayuda a empresas de todos los tamaños a:

- Optimizar los servicios el coste de las TI y la tecnología.
- Apoyar el cumplimiento de las leyes, reglamentos, acuerdos contractuales y las políticas.
- Gestión de nuevas tecnologías de información.

COBIT 5 provee de un marco de trabajo integral que ayuda a las empresas a alcanzar sus objetivos para el gobierno y la gestión de las TI corporativas. Dicho de una manera sencilla, ayuda a las empresas a crear el valor óptimo desde IT manteniendo el equilibrio entre la generación de beneficios y la optimización de los niveles de riesgo y el uso de recursos. COBIT 5 permite a las TI ser gobernadas y gestionadas de un modo holístico para toda la empresa, abarcando al negocio completo de principio a fin y las áreas funcionales de responsabilidad de TI, considerando los intereses relacionados con TI de las partes interesadas internas y externas. COBIT 5 es genérico y útil para empresas de todos los tamaños, tanto comerciales, como sin ánimo de lucro o del sector público. [2]

COBIT 5 ofrece unos principios, prácticas, herramientas analíticas y modelos globalmente aceptados para ayudar a los directivos de negocio y de TI a maximizar la confianza en, y el valor de, sus activos tecnológicos y de información. [2]

Ha sido desarrollado por ISACA, una asociación global, sin ánimo de lucro, que agrupa a más de ciento diez mil profesionales de las disciplinas de la revisión y garantía, la seguridad, la gestión de riesgos y el gobierno corporativo.

COBIT 5 puede ser adaptado a todos los modelos de negocio, entornos tecnológicos, sectores, geografías y culturas corporativas. Puede aplicarse a:

- La seguridad de la información
- La gestión del riesgo
- El gobierno corporativo y la gestión de las TI de la empresa
- Las actividades de revisión y garantía
- La conformidad legal y regulatoria
- El tratamiento de datos financieros o de información sobre RSC

4.6.3 Los 5 Principios de COBIT 5:

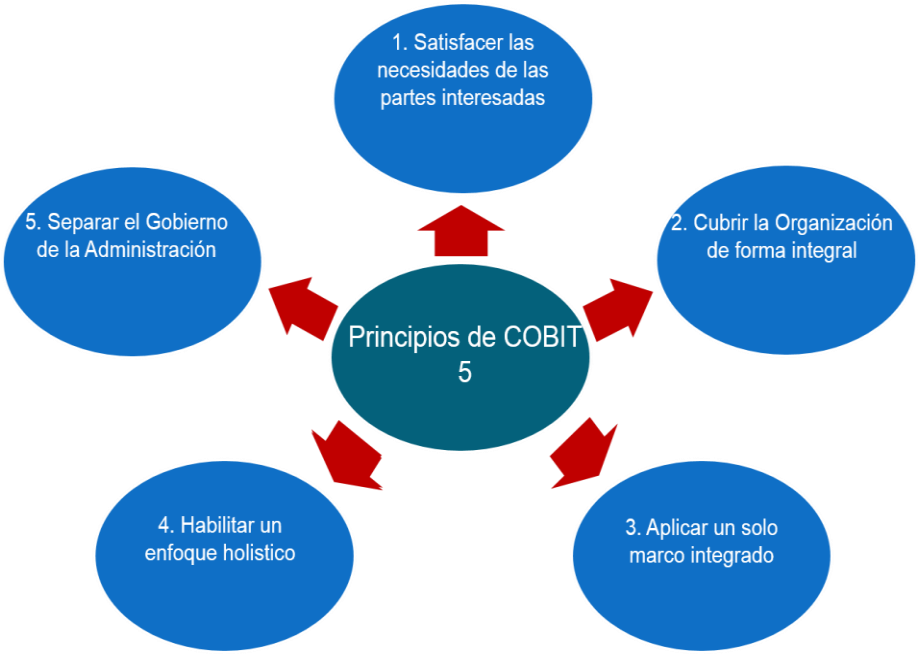


Figura 19. Principios de Cobit 5.
Fuente: COBIT® 5 , Isaca.

1. Satisfacer las necesidades de las Partes Interesadas
2. Cubrir la Compañía de Forma Integral
3. Aplicar un solo Marco Integrado
4. Habilitar un Enfoque Holístico
5. Separar el Gobierno de la Administración.

Juntos, estos cinco principios habilitan a la empresa a construir un marco de gestión de gobierno y gestión efectivo que optimiza la inversión y el uso de información y tecnología para el beneficio de las partes interesadas.

COBIT 5 está organizado en 37 objetivos de control, agrupados en 5 dominios agrupados como lo muestra la figura a continuación:

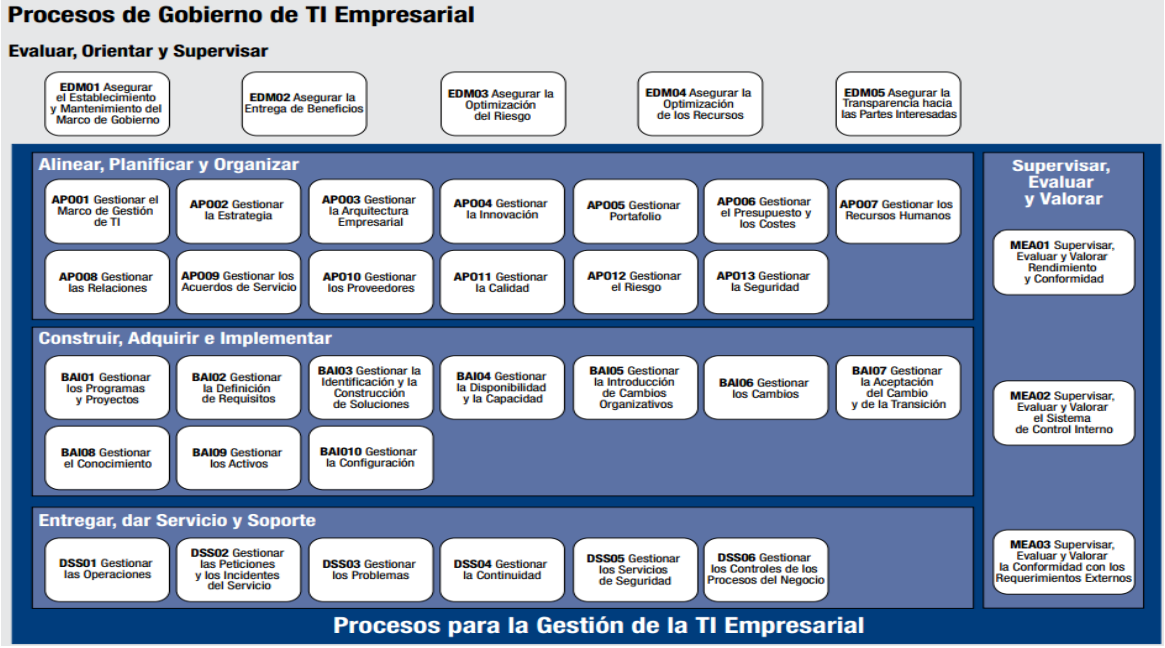


Figura 20. Procesos de Gobierno y Gestión de TI de Cobit 5
Fuente: COBIT® 5, figure 3. © 2012 ISACA® All rights reserved

4.7 La Gestión de Riesgos de TI en el Marco Corporativo

1 El reto actual del profesional de gestión de riesgos de TI se basa en definir un programa continuo, objetivo, repetible y medible, en el que la evaluación de costes, la valoración de activos y las métricas de rendimiento convivan de manera integrada con el resto de requerimientos corporativos.

2 La medida del riesgo, la evaluación y selección de opciones para mitigarlo, gestionando las amenazas que pueden afectar al éxito del negocio, es una disciplina por todos conocida como gestión del riesgo. Sin embargo, la propia definición de riesgo puede variar sustancialmente según la experiencia y formación de cada profesional o del contexto dentro de la organización.

3 Típicamente cuando un profesional de seguridad de la información piensa en riesgo lo hace en términos del impacto que podría suponer en el negocio una pérdida de confidencialidad, integridad o disponibilidad de la información. Sin embargo, y cada día más debido a la madurez de las organizaciones y a los requisitos de cumplimiento, la definición e incluso la catalogación de riesgos es mucho más amplia dentro de lo que la organización considera como riesgos corporativos dentro del marco del gobierno de la empresa.

4 La exposición al riesgo operacional en una organización la podríamos dividir, por ejemplo, en tres grandes áreas: los riesgos inherentes a cualquier entidad, de los procesos que realiza la organización y los relacionados con la estrategia. [18]

4.7.1 Los Riesgos Inherentes a la entidad abarcan los provenientes de:

1 **Los recursos humanos.** Tales como diferencias con los empleados o dependencias de personas clave para la organización, clima social en la compañía y política social, y exposición al riesgo de conflictos con los sindicatos o los representantes de los empleados.

2 **La regulación**. Los requisitos regulatorios suponen un riesgo creciente: es necesario identificar y gestionar las obligaciones de cumplimiento normativo, especialmente en sectores como el financiero, seguros, u hospitalario. Esta gestión dependerá mucho del modelo de negocio o de los países en los que la organización se encuentre. Ejemplos de estas regulaciones son: Sarbanes-Oxley, PCI y DSS.

3 **Los clientes.** Se torna necesaria la identificación de los puntos de conflicto con clientes, de las áreas de la compañía más expuestas al fallo en el servicio al cliente, e, incluso, de los tipos más significativos de riesgo reputacional.

4 **El entorno**. En él se encuadran las situaciones de riesgo más relevantes relacionadas con agentes externos (tormentas, inundaciones, terremotos, pandemias etc.). [18]

4.7.2 Dentro de los riesgos de los procesos de una organización, se podrían incluir:

1 **Fraude interno y externo**. Sería necesario identificar los procesos expuestos al fraude externo basándonos en la experiencia histórica y en entrevistas con los responsables del proceso de negocio; del mismo modo, habría que identificar los procesos susceptibles de fraude interno, como por ejemplo la venta de información confidencial, relaciones con los proveedores, etc.

2 **Pérdidas generadas por una interrupción del negocio.** Sería necesario identificar los procesos expuestos a una interrupción del servicio, es decir aquellos procesos para los cuales una interrupción puede suponer una pérdida financiera por el abandono del servicio al cliente o incluso por penalizaciones

por incumplimiento de pagos o por violación de regulaciones. Este análisis se suele realizar usualmente en el marco de la disciplina de continuidad de negocio.

Pérdidas generadas por errores en la ejecución. Sería necesario identificar las causas más usuales de error en relación con la complejidad y la automatización del proceso: errores humanos, fallos en la integridad TI... Los procesos en los que estos errores podrían impactar son los de pagos, desarrollo de productos financieros y aquellos con fechas de entrega obligatorias. [18]

4.7.3 Riesgos relacionados con la Estrategia

1. **La gestión del cambio.** La innovación y la política de gestión del cambio son parámetros que conducen a la exposición al riesgo. Sería por tanto necesario identificar en una organización como factores de riesgo los nuevos proyectos de TI relativos a cambios significativos o a la implementación de nuevos sistemas, el lanzamiento de productos y la adquisición de compañías.

2. **La política de outsourcing/offshoring.** Las decisiones de externalización de las partes no esenciales del negocio para beneficiarse de economías de escala conducen a nuevos riesgos como la exposición a la ejecución de errores de los proveedores de servicio, a su salud financiera, al riesgo de exponer información confidencial a terceros o los derivados de un plan inadecuado de continuidad de negocio del proveedor. Desde esta perspectiva del concepto de riesgo y su clasificación, cada área de la organización implicada en la identificación, monitorización y gestión de

estos riesgos, y a su vez cada área afectada directamente por una regulación (finanzas, departamentos legales, auditoría, RRHH), puede desarrollar su propia estrategia y metodología para mitigar los riesgos o cumplimientos con las regulaciones. La gestión de riesgos de TI debe responder a esta realidad, ya que se enmarca dentro de la gestión de riesgos de la organización. Su objetivo es proteger la información de la organización y sus sistemas. Adicionalmente, la gestión de riesgos de TI debe considerarse como un programa y no como un proyecto periódico focalizado en controles de seguridad TI.

En esta situación, la gestión de riesgos de TI toma otra perspectiva en la que es necesario crear programas de gestión del riesgo de TI que combinen la gestión de una amplia gama de riesgos específicos relacionados con la tecnología dentro de un programa de gobierno de los riesgos a un nivel superior. Este programa se enfrenta al reto de elaborar unos resultados y controles lo suficientemente flexibles como para poder encajar en este contexto más global de gestión del riesgo, donde las expectativas son más amplias desde el nivel corporativo, en el marco de unos servicios globalizados y con el cada día más extendido uso de proveedores de servicio externos.

La identificación de cualquier riesgo de TI requiere siempre conectar el riesgo a los servicios de TI y, a su vez, estos a los riesgos de negocio. Por ejemplo, el negocio puede enfrentarse a la contingencia de no poder ofrecer determinados servicios debido a la inestabilidad de un sistema TI. Anticiparse a este tipo de situaciones da sentido a la gestión de riesgos de TI más que centrarse en la generación de una serie de medidas puntuales que mitigan ciertos riesgos tecnológicos. [18]

4.8 MECI en el Estado Colombiano.

Este Modelo creó una estructura para el control a la estrategia, la gestión y la evaluación en las organizaciones del Estado, cuyo propósito era orientarlas al cumplimiento de sus objetivos institucionales y a la contribución de estos a los fines esenciales del Estado.

El Presidente de la República como autoridad encargada de fijar las Políticas de Control Interno, según lo dispuesto en las Leyes 87 de 1993 y 489 de 1998, en coordinación con el Consejo Asesor del Gobierno Nacional en materia de Control Interno, ha decidido actualizar el Modelo Estándar de Control Interno establecido mediante Decreto 1599 de 2005 con el fin de fortalecerlo acorde a las normas y tendencias internacionales.

Este Modelo actualizado brinda a las organizaciones una estructura de control cuyo fin último es garantizar razonablemente el cumplimiento de los objetivos institucionales, que sirva a las organizaciones para facilitar la implementación y fortalecimiento continuo de sus Sistemas de Control Interno.

Este Modelo se formuló desde el año 2005, con el propósito de que las organizaciones del Estado obligadas a contar con Sistemas de Control Interno según lo dispuesto en la Ley 87 de 1993, pudieran mejorar su desempeño institucional mediante el fortalecimiento continuo de los controles al interior de la organización y de los procesos de evaluación que deben llevar a cabo las Oficinas de Control Interno, Unidades de Auditoría Interna o quien haga sus veces. Así mismo, para las organizaciones pertenecientes a la Rama Ejecutiva del Orden Nacional, el Modelo Estándar de Control Interno MECI en su actualización, será el medio a través del cual se realizará seguimiento y evaluación a lo dispuesto en el Decreto 2482 de 2012 en cuanto al Modelo Integrado de Planeación y Gestión.[19]

4.8.1 Ámbito de Aplicación

De acuerdo con el artículo 5 de la Ley 87 de 1993, El Modelo Estándar de Control Interno debe ser aplicado por todos los organismos y organizaciones de las Ramas del Poder Público en sus diferentes órdenes y niveles, por la organización electoral, los organismos de control, los establecimientos públicos, las empresas industriales y comerciales del Estado, las sociedades de economía mixta en las cuales el Estado posea el 90% o más de capital social, el Banco de la República y los fondos de origen presupuestal. En consecuencia, dichas organizaciones deberán adaptar este modelo acorde con el tamaño y la naturaleza de las actividades según su objeto legal.[19]

4.8.2 Principios del Modelo Estándar de Control Interno

Los siguientes principios del MECI se constituyen en el fundamento y pilar básico que garantizan la efectividad del Sistema de Control Interno y deben ser aplicados en cada uno de los aspectos que enmarcan el modelo. En consecuencia, las organizaciones en la implementación o revisión o fortalecimiento continuo del Sistema de Control Interno deben incluir estos principios de manera permanente en su actuar:

1- **Autocontrol**

Capacidad que deben desarrollar todos y cada uno de los servidores públicos de la organización, independientemente de su nivel jerárquico, para evaluar y controlar su trabajo, detectar desviaciones y efectuar correctivos de manera oportuna para el adecuado cumplimiento de los resultados que se esperan en el ejercicio de su función, de tal manera que la ejecución de los procesos, actividades y/o tareas bajo

su responsabilidad, se desarrollen con fundamento en los principios establecidos en la Constitución Política.

Capacidad de cada una de las organizaciones para desarrollar y aplicar en su interior métodos, normas y procedimientos que permitan el desarrollo, implementación y fortalecimiento continúo del Sistema de Control Interno, en concordancia con la normatividad vigente.

2- Autorregulación

Capacidad de cada una de las organizaciones para desarrollar y aplicar en su interior métodos, normas y procedimientos que permitan el desarrollo, implementación y fortalecimiento continúo del Sistema de Control Interno, en concordancia con la normatividad vigente.

3- Autogestión

Capacidad de toda organización pública para interpretar, coordinar, aplicar y evaluar de manera efectiva, eficiente y eficaz la función administrativa que le ha sido asignada por la Constitución, la ley y sus reglamentos. La organización deberá establecer políticas, acciones, métodos, procedimientos y mecanismos de prevención, control, evaluación y mejoramiento continuo que permitan dar cumplimiento a cada uno de estos principios, con el propósito de estructurar su Sistema de Control Interno que permita tener una seguridad razonable en el cumplimiento de sus objetivos.[19]

4.8.3 Estructura del MECI en la F.G.N

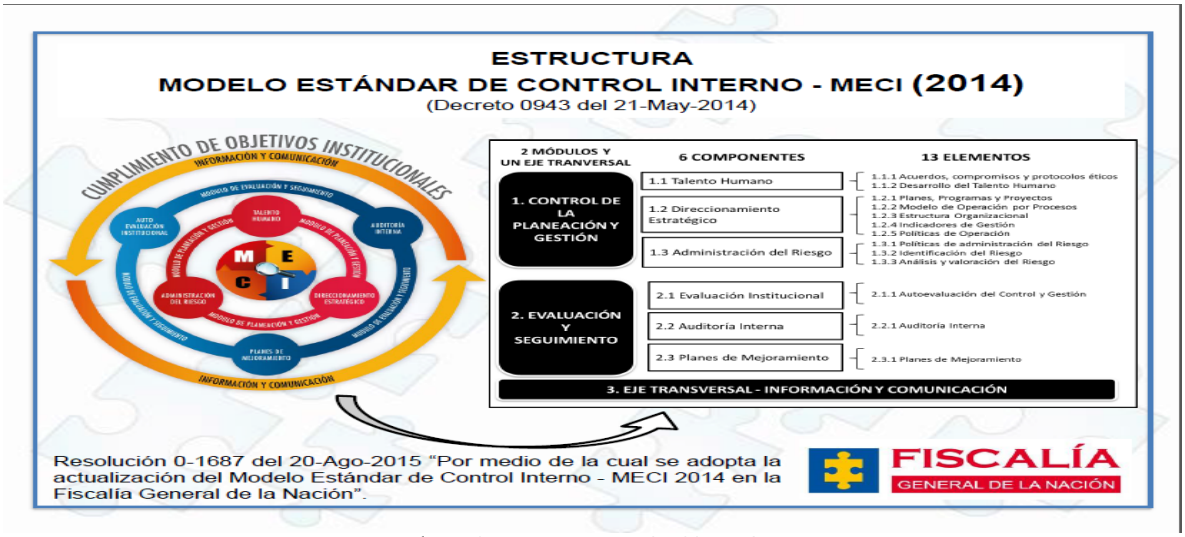


Figura 21. Estructura MECI -2014 FGN

Fuente: Resolución 0-1687 Del 20/08/2015

4.9 Norma ISO 27001 – 27005 Seguridad de la Información

Esta norma cubre todo tipo de organizaciones (por ejemplo: empresas comerciales, agencias gubernamentales, organizaciones sin ánimo de lucro). Esta norma específica los requisitos para establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar un SGSI documentado dentro del contexto de los riesgos globales del negocio de la organización.

Especifica los requisitos para la implementación de controles de seguridad adaptados a las necesidades de las organizaciones individuales o a partes de ellas. El SGSI está diseñado para asegurar controles de seguridad suficientes y proporcionales que protejan los activos de información y brinden confianza a las partes interesadas.[20]

Esta norma adopta el modelo de procesos "Planificar-Hacer-Verificar-Actuar" (PHVA), que se aplica para estructurar todos los procesos del SGSI. La Figura 1

ilustra cómo el SGSI toma como elementos de entrada los requisitos de seguridad de la información y las expectativas de las partes interesadas, y a través de las acciones y procesos necesarios produce resultados de seguridad de la información que cumplen estos requisitos y expectativas.

La adopción del modelo PHVA también reflejará los principios establecidos en las Directrices OCDE (2002)1 que controlan la seguridad de sistemas y redes de información. Esta norma brinda un modelo robusto para implementar los principios en aquellas directrices que controlan la evaluación de riesgos, diseño e implementación de la seguridad, gestión y reevaluación de la seguridad.

Planificar (establecer el SGSI)	Establecer la política, los objetivos, procesos y procedimientos de seguridad pertinentes para gestionar el riesgo y mejorar la seguridad de la información, con el fin de entregar resultados acordes con las políticas y objetivos globales de una organización.
Hacer (implementar y operar el SGSI)	Implementar y operar la política, los controles, procesos y procedimientos del SGSI.
Verificar (hacer seguimiento y revisar el SGSI)	Evaluar, y, en donde sea aplicable, medir el desempeño del proceso contra la política y los objetivos de seguridad y la experiencia práctica, y reportar los resultados a la dirección, para su revisión.
Actuar (mantener y mejorar el SGSI)	Emprender acciones correctivas y preventivas con base en los resultados de la auditoría interna del SGSI y la revisión por la dirección, para lograr la mejora continua del SGSI.

Tabla 1. Estructura del SGSI
Fuente: Norma Técnica Colombiana NTC-ISO-IEC 27001

5. MARCO METODOLOGICO

El marco metodológico empleado en el desarrollo de este proyecto consistió en el diseño de una propuesta de guía para la implementación de un modelo de Arquitectura Empresarial en los entes de control del Estado Colombiano (comenzando por uno de ellos), enfocado en la gestión estratégica de riesgos de TI, utilizando como referencia diferentes modelos y marcos de trabajo, entre ellos, de arquitectura empresarial, TOGAF, ZACHMAN y el modelo que, en esta materia, propone el Gobierno Colombiano a través del Ministerio de tecnologías y las comunicaciones, así como los modelos de gestión de riesgos planteados por Cobit 5.0 e ISO31000. Está compuesto por las siguientes fases:

Fase I – Diagnóstico: Establecer el marco referencial y estudiarlo en detalle a partir de: a) documentación existente (marcos de trabajo, metodologías y buenas prácticas existentes en la literatura sobre el tema), b) antecedentes, contexto y avances en materia de desarrollo de este tipo de herramientas en entidades de control del Estado Colombiano, y c) experiencia de las autoras de este trabajo.

Fase II – Especificación: A partir de los resultados de la fase 1 (objetivo específico 1):

2.1 Definir los requerimientos básicos para el desarrollo de la guía de implementación.

2.2 Extraer del estudio realizado en la fase 1, los componentes y experiencias que aplicarían en mayor grado como fundamento para el diseño de la guía a proponer.

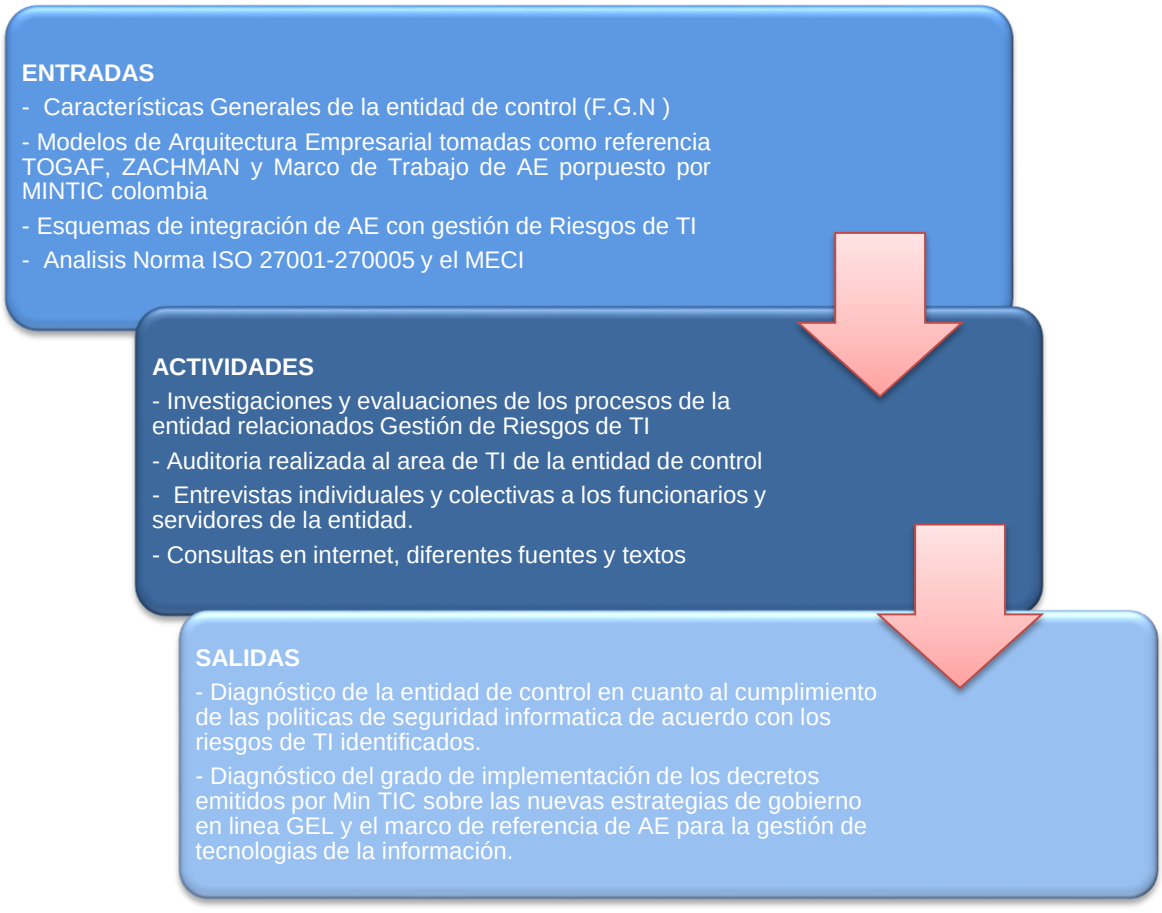
Fase III. Construcción: Diseñar y documentar la guía propuesta a partir del resultado de la fase 2. La guía constará de una serie de sub fases para las que se

especificarán las entradas y salidas de cada una, así como las actividades a realizar dentro de ellas, aplicando los productos de la fase 2.

Fase IV. Presentación de una propuesta de Implementación: como trabajo de campo, presentar y proponer la guía a un ente de control del Estado.

El desarrollo de cada fase, así como las entradas, actividades y salidas que se llevaron a cabo para cada una de ellas, se describen a continuación.

5.1 FASE I: Diagnóstico



Entradas:

Esta fase se desarrolla a partir de la investigación realizada y de la que se presenta un compendio en el marco teórico, la información de las características de una entidad de control, así como la información acerca de los modelos de sistemas de gestión documental y su integración con Gobierno y gestión de TI basados en Cobit 5.

Actividades:

Durante esta fase se realizan investigaciones citadas en el marco de trabajo para tener una visión general del sistema de control interno en la entidad seleccionada: Fiscalía General de la Nación (DCISC-FGN) y un conocimiento general de las actividades de gestión que ésta realiza en el marco en que se desarrolla. (La información mostrada en el transcurso de este documento es solo para fines académicos).

La Fiscalía General de la Nación es una entidad de la rama judicial del **poder público con plena autonomía administrativa y presupuestal**, cuya función está orientada a brindar a los ciudadanos una cumplida y eficaz **administración de justicia**, que investiga los delitos y acusa a los presuntos infractores ante los juzgados y tribunales competentes. Tienen dentro de sus procesos, un proceso de control interno que tiene como función orientar, asesorar, sensibilizar, auditar y realizar seguimiento a los demás procesos para el cumplimiento de las leyes, normas, políticas, procedimientos, planes, programas, proyectos y metas de la Fiscalía General de la Nación y poder recomendar los ajustes necesarios. [17]

La Dirección de control interno en la fiscalía es un instrumento para el buen manejo, custodia, control y aplicación de los recursos públicos en la entidad, evitando de esta manera el detrimento patrimonial sobre los mismos, así como la corrupción

interna por el robo de recursos del Estado por parte de los ordenadores del gasto y su equipo de trabajo.

El Señor Fiscal, junto con su equipo, en el Nivel Central y las diferentes Seccionales son conscientes del compromiso social que representa gestionar recursos administrativos y por ello considera que la gestión que realiza sobre los mismos debe contribuir a la buena administración de justicia, dentro de un ambiente de cero corrupción e impunidad. También entiende que debe ser considerada una entidad que garantice el acceso a la justicia y la efectividad de la acción penal.

Por otra parte, la entidad es vigilada externamente por los siguientes entes de control responsables de ejercer vigilancia y control, estos son:

- Consejo Superior de la Judicatura: (Investiga disciplinariamente a los funcionarios- Fiscales).
- Contraloría General de la República: (Control fiscal).
- Procuraduría General de la Nación: (Investiga disciplinariamente a los funcionarios y empleados públicos).
- Cámara de Representantes- Comisión de Acusación: (Investiga disciplinariamente al Fiscal General de la Nación).

Teniendo como base lo anterior, se procedió a realizar las siguientes actividades dentro de la entidad así:

- Investigaciones y evaluaciones de los procesos de la entidad relacionados Gestión de Riesgos de TI.

- Auditoría realizada al área de TI, la cual tuvo por objetivo: Evaluar la efectividad del control interno y el nivel de seguridad existente en los sistemas de información e infraestructura tecnológica. Actividad que permitió extraer información para la salida de esta fase. Los resultados realizados a

través del informe de auditoría son de carácter confidencial y reserva de la entidad, no obstante para este proyecto fueron tomados con fines educativos, el informe final solo será mostrado al jurado en la sustentación junto con las listas de verificación y papeles de trabajo únicamente como parte del cierre de este trabajo y con las salvedades expresadas al inicio de este documento.

- Entrevistas individuales y colectivas a los funcionarios y servidores de la FGN.
- Consultas en internet en diferentes fuentes y textos que permitieron realizar un diagnóstico inicial de la entidad y plantear una guía para la implementación de un modelo de Arquitectura Empresarial en los entes de control.

Salidas:

De acuerdo con lo descrito anteriormente, se presenta como salida de esta primera fase un diagnóstico inicial de la entidad en lo referente a la Gestión de Riesgos camino a la implementación de arquitectura empresarial establecida por el gobierno a través de diferentes decretos emitidos por Min tic y el Departamento Administrativo de Función Pública en Colombia:

EL proceso de modernización que actualmente afronta la entidad obligó a la reformulación de las estrategias para el logro de los objetivos misionales; en este sentido se encuentran 14 objetivos estratégicos, sobre los cuales se hace la presentación de los siguientes:

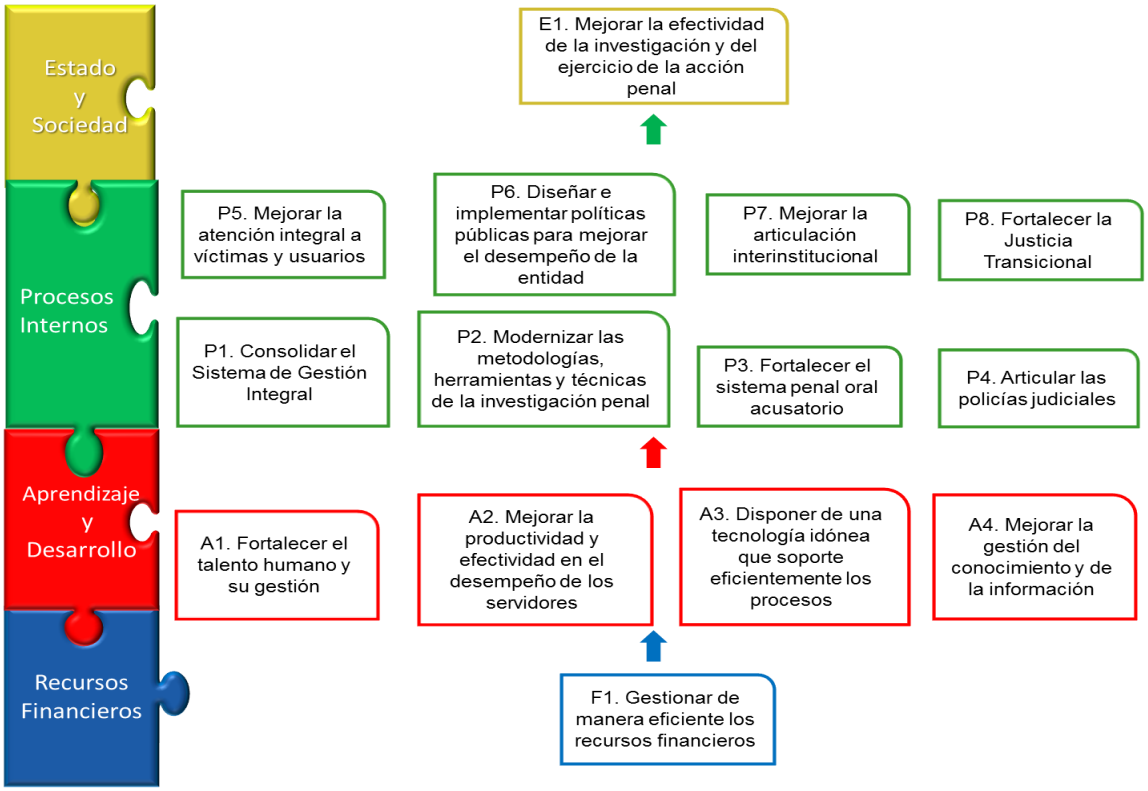


Figura: 22 Objetivos Organizacionales FGN

Fuente: http://www.fiscalia.gov.co/colombia/wp-content/uploads/2013/03/DireccionamientoEstrategico2013_2016.pdf

Teniendo en cuenta que la tecnología debe ser propia de la institución, no es viable la tercerización, en el entendido que el manejo de la información es de carácter reservado y solo obedece a la competencia institucional, eso significa contar con un componente robusto propio, a nivel hardware y software.

Un tercero administrando no tiene una visión clara de los verdaderos objetivos corporativos de la entidad y será solo un solucionador de problemas en el momento.

Así mismo, no tendrá una perspectiva de las implicaciones de un problema relacionado con la misión institucional, de una perdida de información o de una modificación de una base de datos relacionadas con noticias únicas criminales (NUC) o en su mínima expresión una interrupción del servicio.

Estado Actual De la Entidad

	PROCESOS CORPORATIVOS	CIRCUITO ADAPTACION			CIRCUITO REGULACIÓN		
		Función de Politicas	Función de Afuera y el Mañana	Función Interna y el Ahora	Función de Monitoreo	Función Interna y el Ahora	Función de Coordinación
X	Disponer de una Tecnología Idónea que Soporte Eficientemente los Procesos			X4	X3	X2	X1
Y	Modernizar las Metodologias, Herramientas y Técnicas de la Investigación Penal						Y1
Z	Fortalecer el Sistema Penal Oral Acusatorio						Z1

X1: Representa el procedimientos, caracterización del proceso Gestión tecnológica, Matriz de interacción procesos, Matriz de Riesgos institucional y Matriz de Riesgos de Gestión y Mapa de Riesgos de Corrupción.

FGN-12.6-P-01 ATENCIÓN DE REQUERIMIENTOS V01,

FGN-14.2-F-04 CARACTERIZACION GESTION TECNOLOGICA V01

MATRIZ DE INTERACCIÓN POR PROCESOS 2016-V3.

FGN-14.2-F-13 MAPA DE RIESGOS GESTIÓN TECNOLÓGICA

X2: Representa el listado maestro de documentación Externa y Normatividad en la entidad.

FGN-14 2-F-01 LMDEN-GESTION TECNOLOGICA. V01.XLSX (DECRETOS Y ESTANDARES).

MATRIZ ANÁLISIS CONTROL INTERNO - FGN.XLSX (FORMATOS E INSTRUCTIVOS)

X3: Representa los indicadores de gestión

INDICADORES.XLSX

POLÍTICA ADMINISTRACIÓN DE RIESGOS 2015.DOCX (EXIGENCIA MECI)

PROCEDIMIENTO OBLIGATORIO DE AUDITORIA INTERNA FGN-18-P-01 VERSIÓN 2

X4: Representa el mapa de riesgos de gestión tecnológica y de corrupción

FGN-14.2-F-13 MAPA DE RIESGOS GESTIÓN TECNOLÓGICA

Y1: representa la Matriz de flujo de información y comunicación con cada uno de los procesos de la entidad

MATRIZ Y FLUJOS DE INFORMACIÓN Y COMUNICACIÓN

MATRIZ DE INTERACCIÓN POR PROCESOS 2016-V3

Z1: representa la Matriz de flujo de información y comunicación con cada uno de los procesos de la entidad

MATRIZ Y FLUJOS DE INFORMACIÓN Y COMUNICACIÓN

MATRIZ DE INTERACCIÓN POR PROCESOS 2016-V3

Diagnóstico Según Modelo Viable

Acorde con la apreciación de las autoras de este documento y en su opinión propia más no en nombre de la entidad y producto de lo expresado por los encuestados (encuesta solo fines educativos para la realización de este proyecto)**:**

- ✓ En ninguno de los procesos de la entidad se observa evidencia de estar mirando hacia el futuro, faltan mecanismos de anticipación y evaluación por escenarios (**función afuera y el mañana**).
- ✓ En ninguno de los procesos se observa un mecanismo formal para que la alta dirección pueda tomar decisiones con información resumida, de esta forma es muy difícil lograr **políticas e identidad.**
- ✓ En los procesos Y y Z, no se observa una función clara de **monitoreo** por medio de indicadores, no se evidencian políticas organizacionales para la administración del riesgo, las existentes obedecen a estándares que no permiten alcanzar los objetivos, no se observa la existencia de la **función interna y el ahora.** El circuito de **regulación** está **incompleto** y el de **adaptación** es **ausente** para Y y Z.
- ✓ Para que el sistema se adapte al entorno se requiere mirar hacia adelante, por medio de la implementación de la función **afuera y el mañana.**

Diagnóstico de la Evaluación del Control Interno

- ✓ Está orientado al control de los recursos (Aplicar toda la normatividad de la contratación estatal).
- ✓ Sujeto a las normas, las leyes y los reglamentos.
- ✓ Transparencia en las actuaciones de los servidores públicos, cero anticorrupción.
- ✓ Control Fiscal, de legalidad, de resultados.

- ✓ Participación ciudadana.

Cuando Hay crisis en la Entidad estos son los Resultados expresados por los servidores entrevistados:

- ✓ Se buscan responsables del proceso.
- ✓ Se aplican las sanciones disciplinarias y legales al servidor (funcionario) de acuerdo con los daños o el detrimento patrimonial.
- ✓ Se aumentan más los controles normativos (Crece la lista) no hay flexibilidad.
- ✓ Se pierde credibilidad en el área o proceso, llegando al extremo de solicitar intervención de los entes de control externos.
- ✓ Se cuestiona la labor de todo el equipo de trabajo dentro del proceso.
- ✓ No hay trabajo en equipo, cada servidor (funcionario) se va para el lado que le convenga (hacen notar su jerarquía).
- ✓ No se gerencia la incertidumbre, se limita.
- ✓ Los errores deliberados no son permitidos.
- ✓ Se observaron situaciones en que los servidores (funcionarios) no hacen más de lo se les establece en el manual de funciones, no hay valor agregado que ayude a fortalecer las áreas o procesos.
- ✓ En la elaboración de la matriz de riesgos de los procesos, no hay participación de las seccionales, solo son diseñadas por la oficina de planeación.
- ✓ Para presentar propuestas o proyectos debe ser un servidor con receptividad en la alta dirección.

Análisis Interno de la entidad de control

Fortalezas

1. Funcionarios de las TIC, con experiencia, alto nivel de formación profesional y compromiso en sus respectivos roles.
2. Desarrollo y mantenimiento interno de sistemas de información.
3. Cobertura nacional de las comunicaciones a nivel de video, voz y datos.
4. Alto porcentaje de actualización de la plataforma de cómputo para puestos de trabajo a nivel nacional.
5. Inversiones en tecnología en las dos últimas vigencias.
6. Orientación estratégica que contempla el fortalecimiento tecnológico de la misma.

Debilidades

1. Estructura de planta reducida frente a la demanda de servicios en los distintos procesos de TIC.
2. Desactualización documental frente a los nuevos procesos incorporados en las TICs.
3. Primacía del trabajo por áreas funcionales sobre el trabajo por procesos.
4. Falta de énfasis en la implementación del Plan Maestro de Tecnología para todas las áreas de la Entidad.
5. Falta de articulación de roles y funciones con los procesos de TIC´s
6. Conocimientos insuficientes a nivel legal, técnico y administrativo relacionados con la contratación de TIC.
7. Falta de actualización del Plan de Contingencia y del Plan de Recuperación de Desastres.
8. Falta de programas de sensibilización en la gestión adecuada de los procesos de las Tecnologías de la Información y las Comunicaciones.

9. Algunas herramientas tecnológicas desactualizadas y obsoletas de los Sistemas de Información.
10. Insuficiente divulgación a otras unidades o áreas acerca de las directrices de la entidad en materia de TIC.
11. Ausencia de una correcta caracterización del inventario de los activos informáticos.
12. Plan Maestro de Tecnología desactualizado

Análisis Externo

Oportunidades

1. Apoyo del Gobierno Nacional en la gestión de TICs a través del programa de Gobierno en Línea.
2. Desarrollos tecnológicos disponibles en el mercado nacional e internacional.
3. Apoyo del Gobierno Nacional y de organismos de cooperación internacional por mejorar los resultados en la administración de justicia.
4. TIC como prioridad en el alto Gobierno de la entidad.
5. Rezago presupuestal frente a lo programado en el PMTI, Marco de Gasto de Mediano Plazo y Presupuesto anual

Amenazas

1. Desarrollos tecnológicos disponibles en el mercado nacional e internacional.
2. No tener en cuenta o no estar actualizado sobre los cambios en la legislación del uso de tecnologías.
3. No contar con la disponibilidad presupuestal suficiente para la adquisición de tecnologías de punta y proyectos TIC.
4. Falta de inclusión del líder funcional en la Supervisión de Contratos, Políticas de desarrollo e implementación del Programa de Modernización de la Entidad.

5. Apoyo de los funcionarios de otras áreas que cumplen con funciones relacionadas con TIC.

Diagnóstico de la Cadena Valor Actual Vs Cadena de Valor Deseada

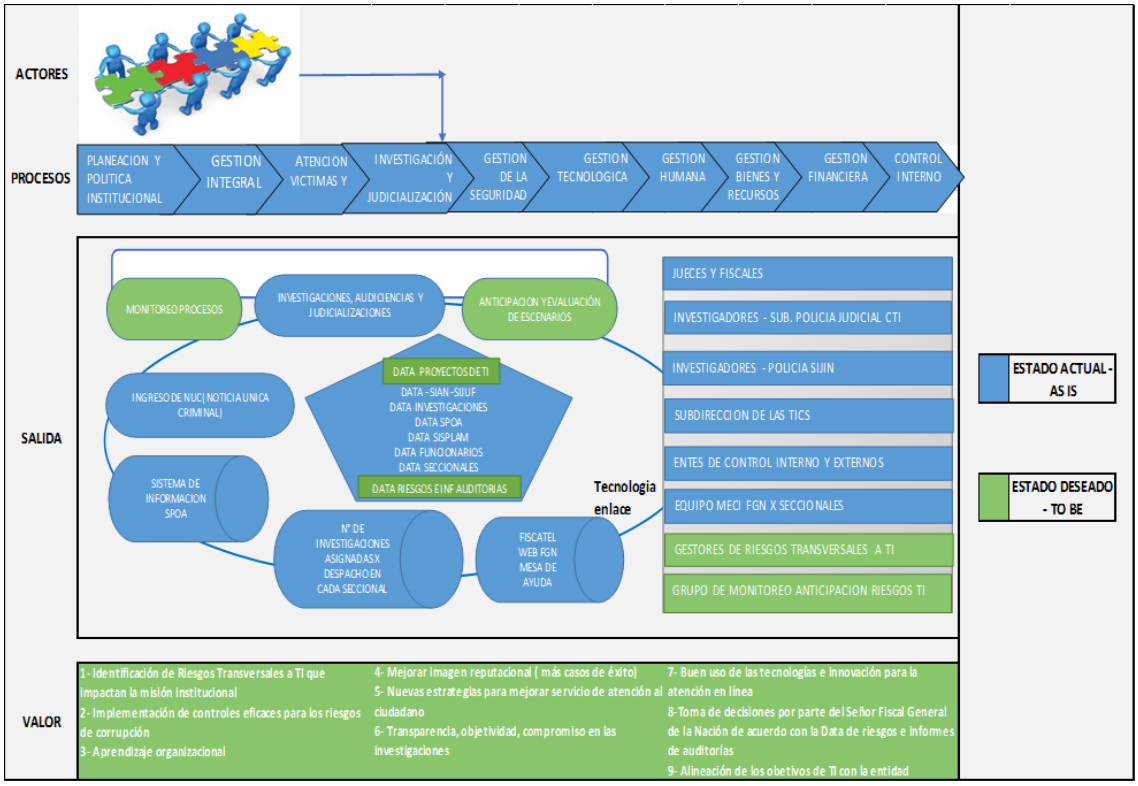


Figura 23: Estado Actual Vs Deseado de la Entidad de control

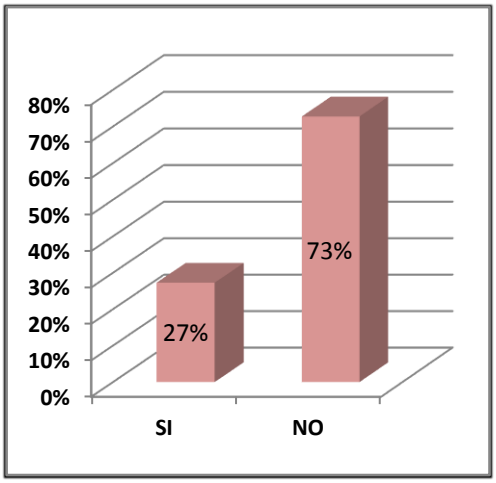
Fuente: iniciativa propia

Resultado de la encuesta aplicada a los Servidores/funcionarios del Área de TI de la Entidad

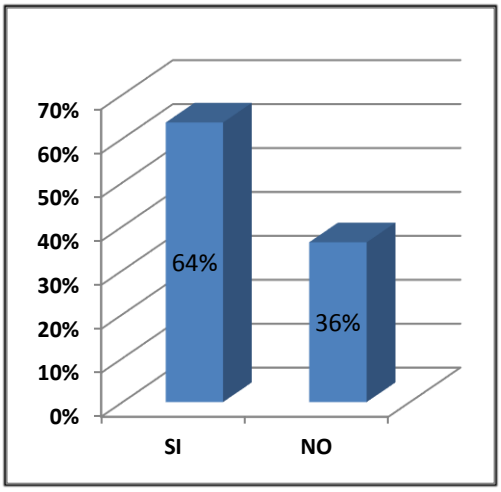
Se realizó una encuesta para evaluar la percepción que tiene el área de TI sobre la arquitectura actual de la entidad; la encuesta realizada y su cuadro técnico (población, etc.) se encuentra en el **ANEXO 1.**

A continuación se observan los resultados de la misma: **Aspectos Generales de Seguridad**

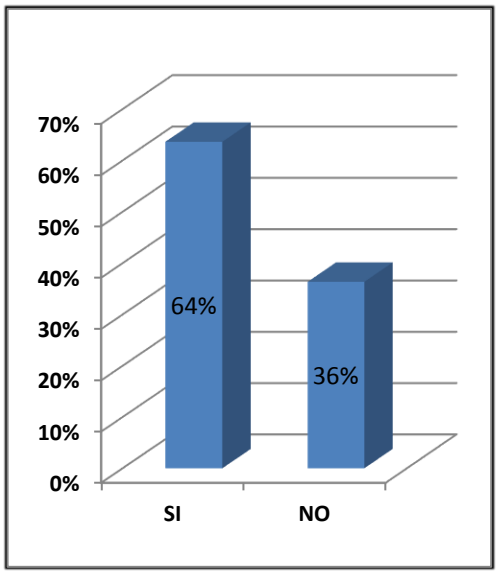
1. Conoce usted cuales son los objetivos institucionales?



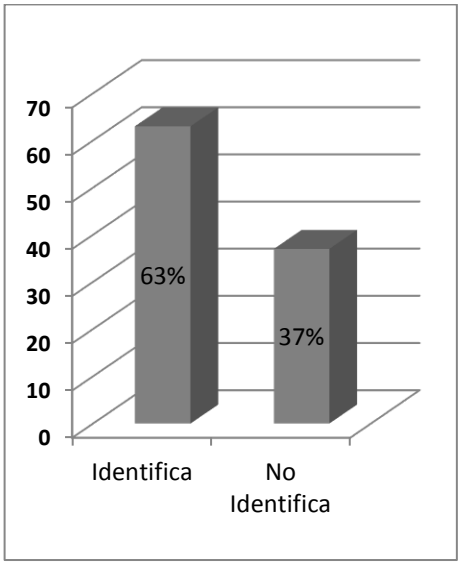
2. Conoce usted cuales son los objetivos de T.I en la entidad?



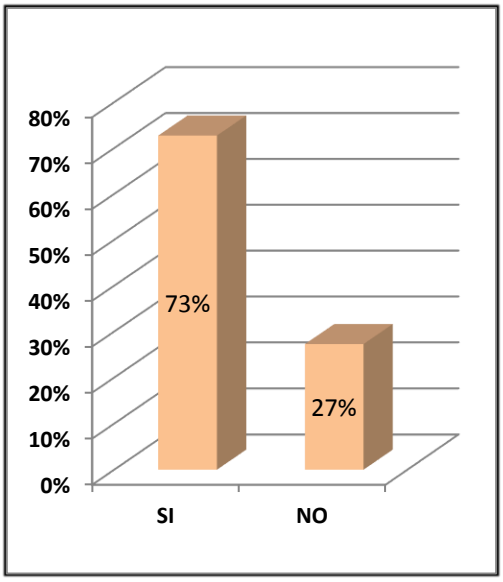
3. Conoce que es el SGSI?



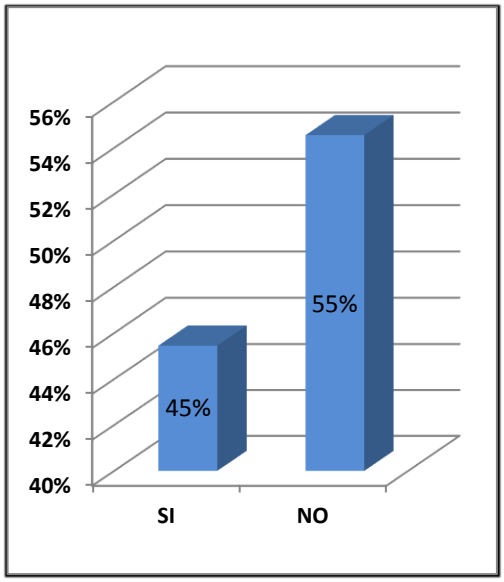
4. Mencione tres riesgos que puedan afectar la confidencialidad, integridad y disponibilidad de la información en su área, en el entendido de cómo no debería funcionar un sistema de información? (7 servidores identificaron riesgos y 4 no identificaron riesgos)



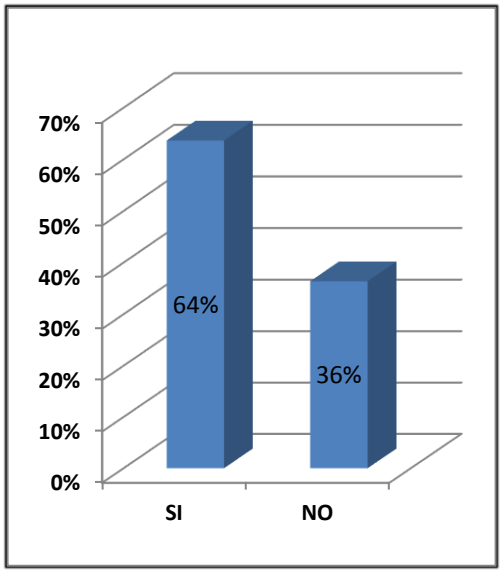
5. Conoce usted cual es el objetivo principal de implementar la política de la seguridad de la información en la entidad?



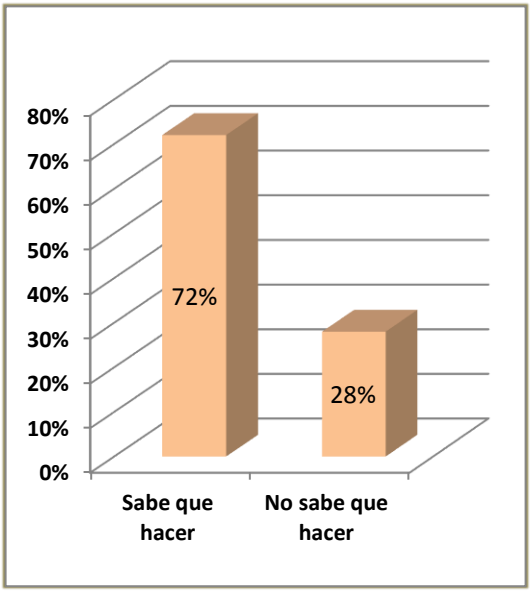
6. Hace usted copias de respaldo de la información y de los sistemas de información?



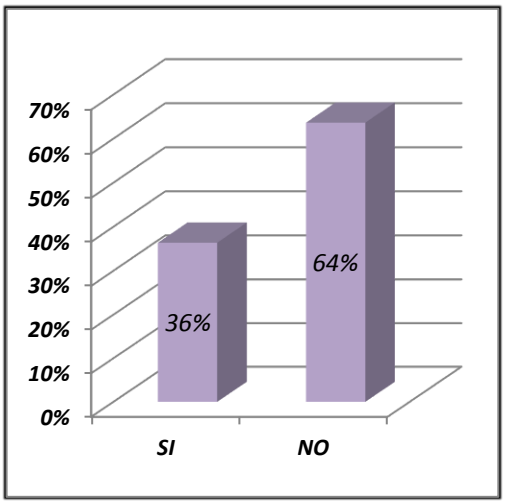
7. Existe una política de respaldo de la información definida por la entidad?



8. Como reaccionaria usted ante una falla?

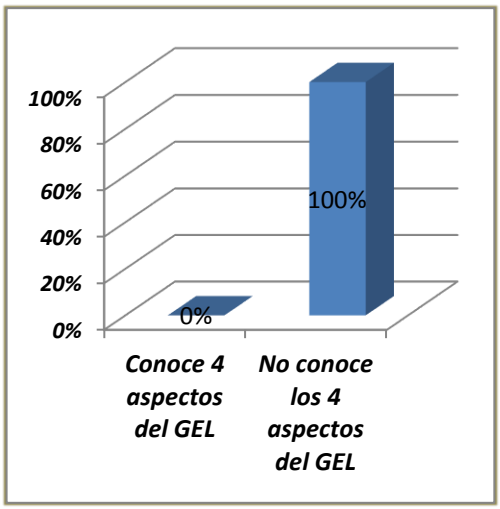


9. Cree usted que los riesgos son cambiantes en un entorno VICA (volátiles, inciertos, complejo y ambigüos)?



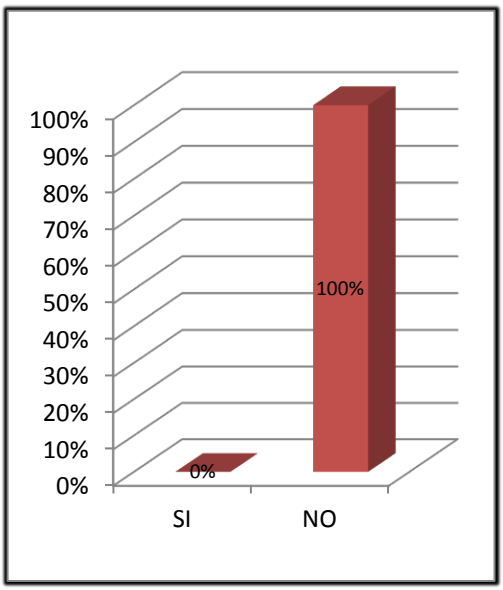
Aspectos Generales de Gobierno en Línea

10. Mencione cuáles son los aspectos en los que se enfoca la estrategia de Gobierno en Línea según MinTic[3]?

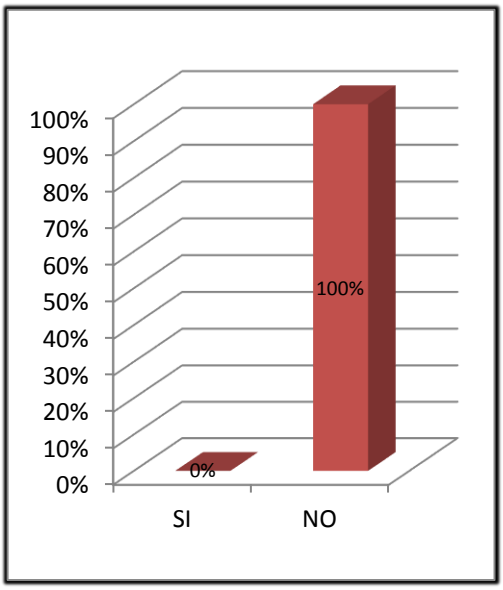


[3] *"Aspectos sobre los cuales se enfoca la Estrategia de Gobierno en Línea colombiana: TIC para el servicio, TIC para el gobierno abierto, TIC para la gestión y TIC para la seguridad y privacidad de la información."*

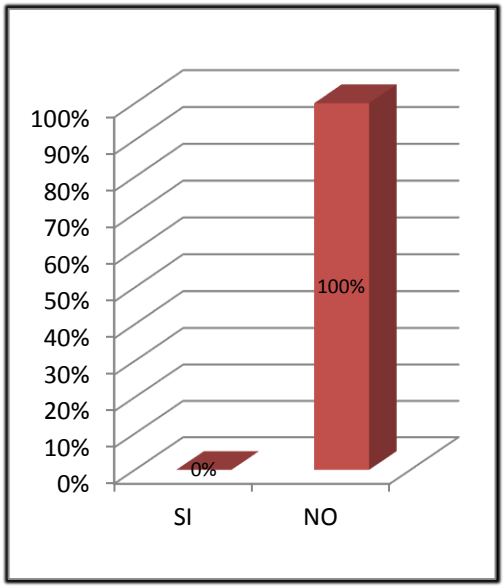
11. ¿Conoce usted que es la arquitectura empresarial (AE) de Tecnología de la Información?



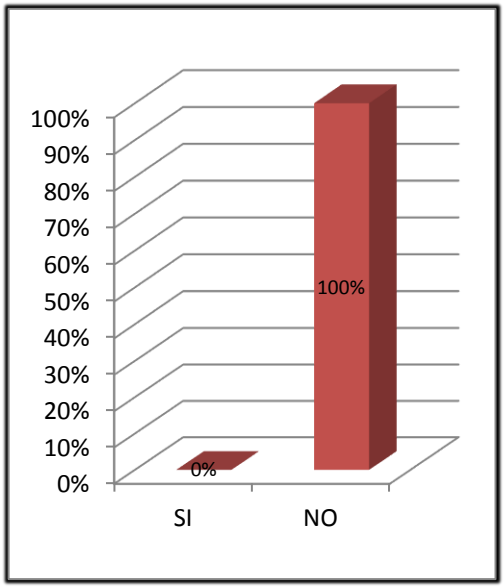
12. ¿Conoce usted el modelo de AE(arquitectura Empresarial) que debe ser aplicado en la entidad según MINTIC?



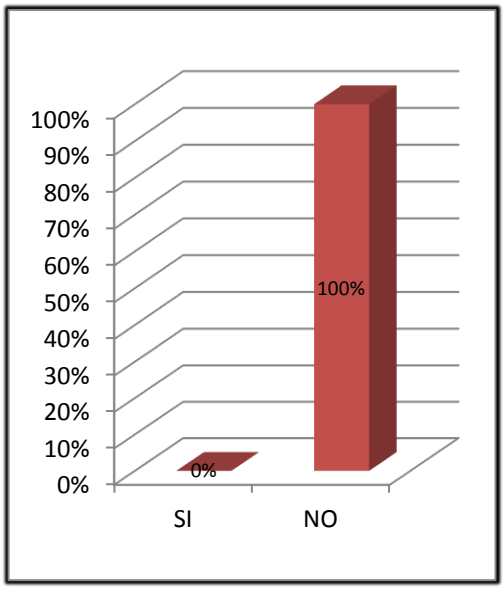
13. Conoce usted el comité de gobierno en línea de la entidad?



14. En la entidad realizan análisis de Riesgos de TI en todos los procesos?



15. En la elaboración de la matriz de riesgos se tienen en cuenta a las seccionales?



Por otro lado, se tomó con insumo para este proyecto información de la última auditoría realizada a la subdirección de las TICs en la entidad del 18 al 28 de octubre de 2016 donde se identificaron las siguientes debilidades:

- ✓ La política de la seguridad informática se constituye en la primera línea de defensa de la entidad, frente a ataques y amenazas sobre la disponibilidad, confidencialidad e integridad de los activos de información, ya que su construcción debe estar basada en un proceso de continuo análisis de riesgos, así como en la implementación adecuada de controles con el fin de mitigar posibles materializaciones del mismo.[4] Así mismo, se debe considerar que la gestión de riesgos, es un proceso que incluye la prevención, detección y respuesta a incidentes, mantenimiento, auditorias y revisión continúas.

[4] Componente Administración del Riesgo MECI -2014: se convierte en una herramienta fundamental para las entidades, en el entendido de que su correcta aplicación tiene como resultado latente, el evitar la ocurrencia de hechos o situaciones que afecten o entorpezcan la gestión de las entidades.

Si bien en el Proceso de Gestión Tecnológica se tienen identificados 2 riesgos de gestión y 1 de corrupción, cuando se analiza el mapa de riesgos institucional del 10 de agosto de 2016, solo se identifica un riesgo de tipo operativo, para el proceso de gestión tecnológica, relacionado con el SPOA (Sistema Penal Oral Acusatorio), dejando ver que muchos de los riesgos que puedan identificarse con relación a la seguridad de la información no han sido previstos por los líderes de los procesos. Así las cosas, se debe revisar un posible incumplimiento con lo establecido en el numeral 9, del artículo 39 del decreto 016 de 2014, el cual establece como una de las funciones de la Subdirección de TICs *"Gestionar, atender, proponer e implementar las políticas y acciones relativas a la seguridad y oficialidad de la información y de la plataforma tecnológica de la Fiscalía General de la Nación*"; en concordancia con lo establecido en la Resolución 0-4004 artículo 6 numeral 3, literal b, c y d.

Esta situación, no permite adoptar acciones preventivas frente a posibles amenazas o ataques contra la seguridad de la información que es generada y utilizada en los diferentes procesos de la entidad, así como, a su confidencialidad e integridad.

La entidad tiene como objetivo principal en la resolución 0-1261 del 23 de julio de 2014, el establecimiento de directrices y buenas prácticas para los sistemas de información, en consideración a lo señalado en el artículo 39, numeral 1 del decreto ley 016 de 2014 donde se determina que le corresponde a la Subdirección de Tecnologías de la Información y las Comunicaciones " *Asesorar al Fiscal General de la Nación en la definición de políticas, planes, programas y procedimientos relacionados con el uso de las tecnologías de la información y las Comunicaciones que contribuya a incrementar la eficiencia y eficacia en las diferentes dependencias de la entidad, así como garantizar las calidad en la prestación de los servicio*". De igual manera para adelantar las acciones pertinentes de acuerdo con las estrategias de Gobierno En Línea – GEL, establecidas en el artículo 230 de la ley 1450 de 2011 que dice: "***Artículo 230. Gobierno en Línea como Estrategia de Buen Gobierno.*** *Todas las entidades de la administración pública deberán adelantar las acciones*

señaladas por el Gobierno Nacional a través del Ministerio de las Tecnologías de la Información y las Comunicaciones para la estrategia de Gobierno en Línea.

Esta estrategia liderada por el Programa Gobierno en Línea contemplará como acciones prioritarias el cumplimiento de los criterios establecidos al respecto, así como, las acciones para implementar la política de cero papel, estimular el desarrollo de servicios en línea del Gobierno por parte de terceros basados en datos públicos, la ampliación de la oferta de canales aprovechando tecnologías con altos niveles de penetración como telefonía móvil y televisión digital terrestre, la prestación de trámites y servicios en línea y el fomento a la participación y la democracia por medios electrónicos.

El Gobierno implementará mecanismos que permitan un monitoreo permanente sobre el uso, calidad, nivel de satisfacción e impacto de estas acciones."

Conforme lo anteriormente expuesto, se muestran los siguientes resultados:

Se evidenció, que existen sistemas de información, tales como, [5]SRAF, SIG y SISAC entre otros, que han sido desarrollados por la Dirección Nacional del Cuerpo Técnico de Investigaciones - CTI, que aún no están bajo la gobernabilidad de la Subdirección de Tecnologías de la Información y de las Comunicaciones; por lo tanto, se incumple con lo establecido en el artículo 8, de la resolución 0-1261 del 23 de julio de 2014, el cual dice: *"La Subdirección de Tecnologías de la Información y de las Comunicaciones realizará todas las actividades tendientes a lograr el gobierno de los Sistemas de Información a fin de que los sistemas que han sido construidos por las dependencias de la Fiscalía General de la Nación, se incorporen y se integren a los sistemas misionales y/o de apoyo, ya institucionalizados"*

[5] SRAF: Sistema para el Registro de Armas de Fuego en la entidad. SIG: Sistema de Información para la Gestión Técnico investigativa. SISAC: Sistema de información Sección Análisis Criminal.

En consecuencia, se puede concluir que no se han adoptado en su totalidad las buenas prácticas para fortalecer el desarrollo y mantenimiento der los sistemas de información.

Seguidamente, se elaboró el modelo de gobierno y gestión de TI en la F.G.N, el cual se muestra a continuación:

Modelo de Gobierno y de Gestión de TI en la entidad (Arquitectura de Negocio)

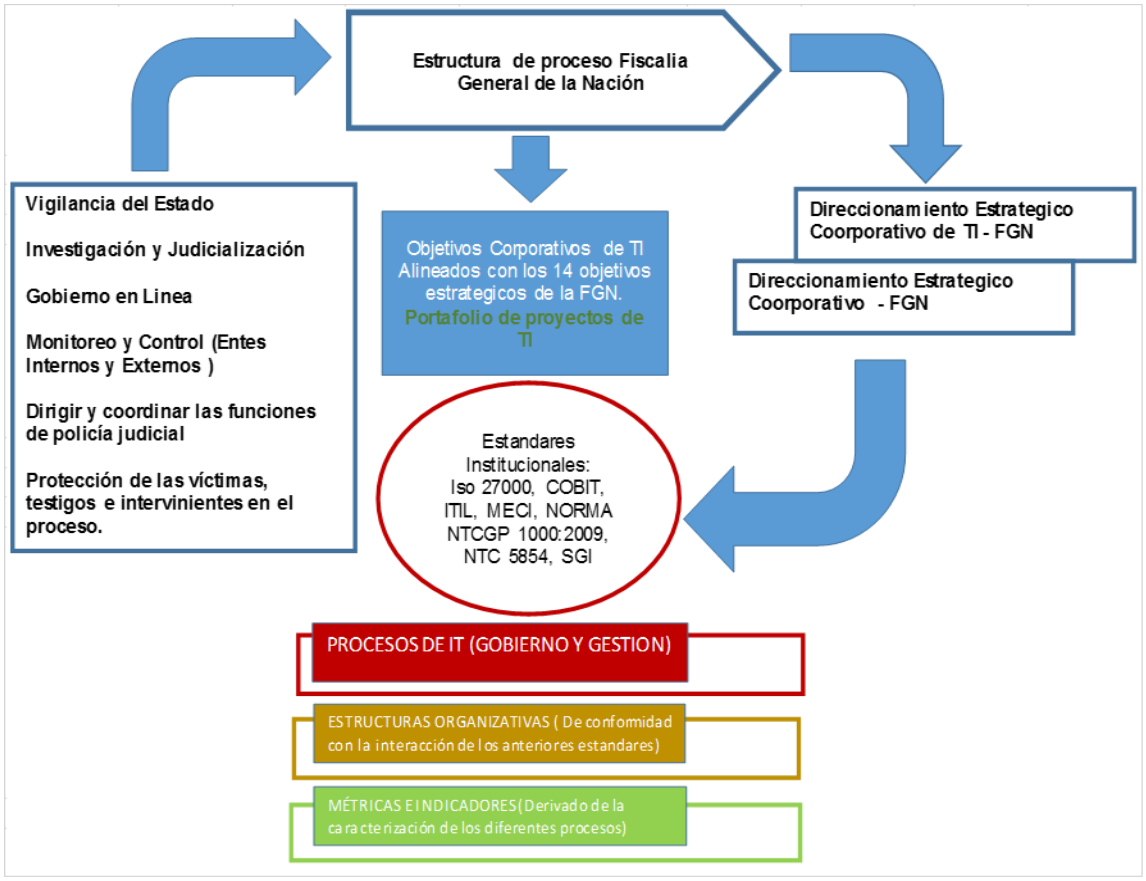


Figura 24: Modelo G. y G de TI en la entidad de control

Fuente: Iniciativa propia

Actualmente, la entidad a tenidos cambios estructurales con cambios en los objetivos estratégicos organizacionales, los cuales se describen a continuación:

- ✓ **Gestionar de manera eficiente los recursos financieros**
- ✓ Fortalecer el talento humano y su gestión
- ✓ Mejorar la productividad y efectividad en el desempeño de los servidores
- ✓ **Disponer de una tecnología idónea que soporte eficientemente los procesos**
- ✓ **Mejorar la gestión del conocimiento y de la información**
- ✓ Consolidar el Sistema de Gestión Integral
- ✓ **Modernizar las metodologías, herramientas y técnicas de la investigación penal**
- ✓ Fortalecer el sistema penal oral acusatorio
- ✓ Articular las policías judiciales
- ✓ Mejorar la atención integral a víctimas y usuarios
- ✓ Diseñar e implementar políticas públicas para mejorar el desempeño de la entidad
- ✓ Mejorar la articulación interinstitucional
- ✓ Fortalecer la Justicia Transicional
- ✓ Mejorar la efectividad de la investigación y del ejercicio de la acción penal

Y como objetivos de TI, la entidad tiene los siguientes:

- ✓ Asesorar y dar apoyo en la planeación
- ✓ Operación y control de los procesos de TIC en la FGN
- ✓ Proporcionar servicios informáticos de calidad, seguros y eficientes, bajo procedimientos estandarizados
- ✓ Incrementar la calidad, la productividad y generar mejores servicios para el ciudadano

Para el análisis y apuntando a los objetivos de este proyecto se tomaron los siguientes objetivos de la entidad:

1- **Gestionar de manera eficiente los recursos financieros**

2- **Disponer de una tecnología idónea que soporte eficientemente los procesos.**

3- **Mejorar la gestión del conocimiento y de la información.**

4- **Modernizar las metodologías, herramientas y técnicas de la investigación penal.**

Analizados los objetivos estratégicos seleccionados (análisis que se adjuntan al proyecto como anexos), se propone la correlación con las siguientes metas corporativas de COBIT 5 así:

Procesos Claves para extraer los principales para la entidad de control en estudio

EDM03: Asegurar la optimización del riesgo

APO03: Gestionar la Arquitectura Empresarial

APO12: Gestionar el Riesgo

APO13: Gestionar la seguridad

BAI01: Gestionar los programas y proyectos

BAI07: Gestionar la aceptación del cambio y de la transición

DSS05: Gestionar los servicios de seguridad

DSS06: Gestionar los controles de los procesos del negocio

MEA02: Supervisar, evaluar y valorar el sistema de control interno

MEA03: Supervisar, evaluar y valorar la conformidad con los requerimientos externos.

Principales Procesos Seleccionados de COBIT 5.0 Para Aplicar en la entidad

APO03: Gestionar la Arquitectura Empresarial

APO12: Gestionar el Riesgo

DSS06: Gestionar los controles de los procesos del negocio

MEA03: Supervisar, evaluar y valorar la conformidad con los requerimientos externos.

Estos procesos seleccionados se detallan en la fase II de este proyecto.

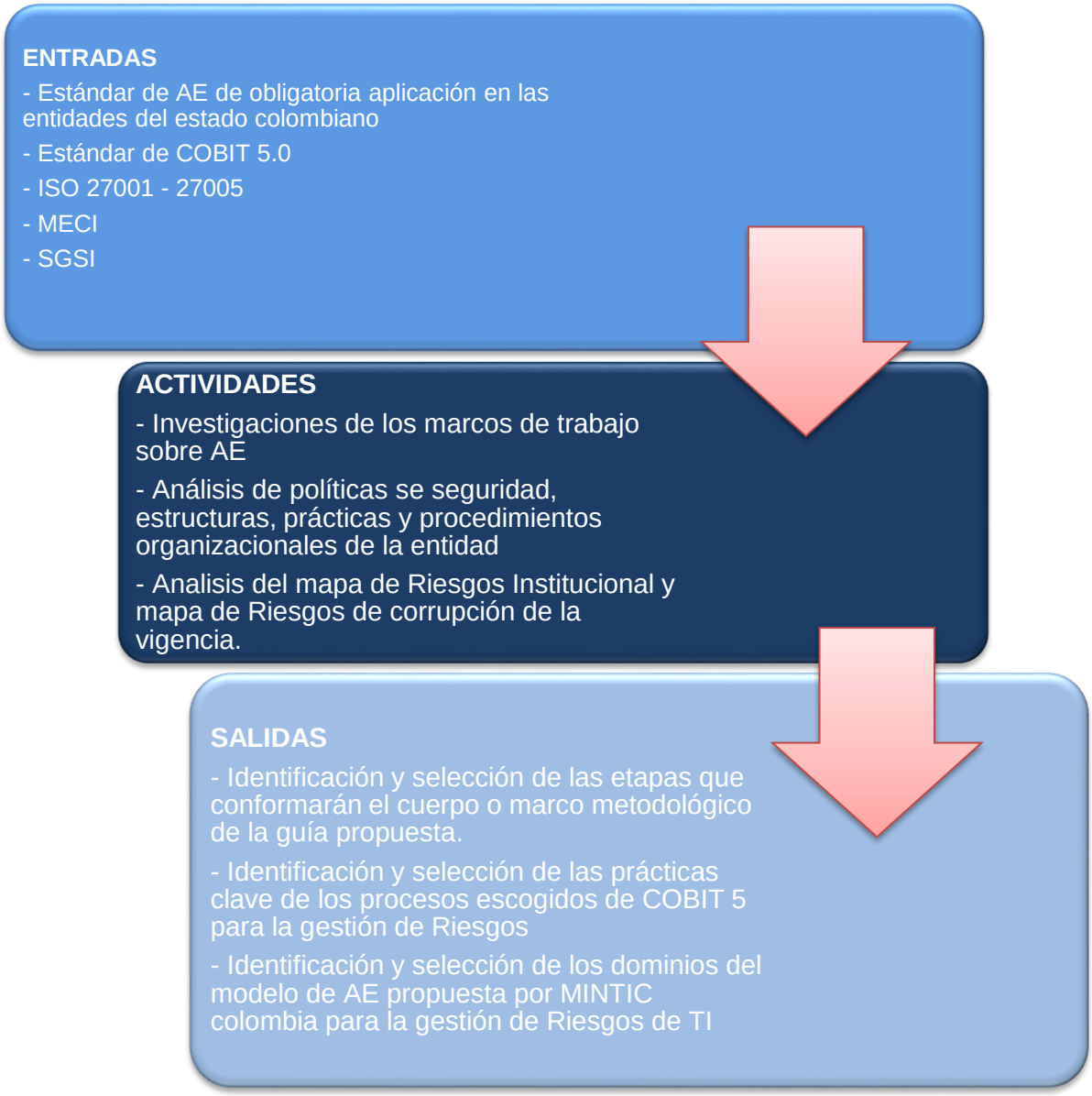
5.2 Fase II – Especificación:

A partir de los resultados de la fase 1 (objetivo específico 1):

5.2.1 Definir los requerimientos básicos para el desarrollo de la guía de implementación.

5.2.2 Extraer del estudio realizado en la fase 1,

Los componentes y experiencias que aplicarían en mayor grado como fundamento para el diseño de la guía de implementación.



Procesos seleccionados en COBIT 5.0 de acuerdo con análisis realizado en la entidad para la implementación de Arquitectura Empresarial según lo establecido por MINTIC.

APO03: GESTIONAR LA ARQUITECTURA EMPRESARIAL (ENTIDAD DE CONTROL)

Descripción del Proceso

Establecer una arquitectura empresarial en la Fiscalía General de la Nación compuesta por los procesos de negocio, la información, los datos, las aplicaciones y las capas de la arquitectura tecnológica de manera eficaz y eficiente para la realización de las estrategias de la empresa y de TI mediante la creación de modelos clave y prácticas que describan las líneas de partida y las arquitecturas objetivo. Definir los requisitos para la taxonomía, las normas, las directrices, los procedimientos, las plantillas y las herramientas y proporcionar un vínculo para estos componentes. Mejorar la adecuación, aumentar la agilidad, mejorar la calidad de la información y generar ahorros de costes potenciales mediante iniciativas tales como la reutilización de bloques de componentes para los procesos de construcción.

Declaración del Propósito del Proceso

Representar a los diferentes módulos que componen la entidad y sus interrelaciones, así como los principios rectores de su diseño y evolución en el tiempo, permitiendo una entrega estándar, sensible y eficiente de los objetivos operativos y estratégicos.

El proceso seleccionado apoya la consecución de un conjunto de principales metas de TI:

Metas de TI con sus respectivas Métricas Relacionadas

- **01 Alineamiento de TI (subdirección de las TICs) con el direccionamiento estratégico de la entidad**

1. Porcentaje de las metas y requerimientos estratégicos de la entidad soportados por las metas estratégicas para TI.
2. Nivel de satisfacción de las partes interesadas con el alcance del portafolio de programas y servicios planeados.
3. Porcentaje de los facilitadores de valor de TI mapeados con facilitadores de valor del negocio

- **09 Agilidad de las TI**

1. Nivel de satisfacción del Fiscal General de la Nación con la capacidad de respuesta de TI a nuevos requerimientos.
2. Número de procesos de negocio críticos soportados por infraestructuras y aplicaciones actualizadas.
3. Tiempo medio para convertir los objetivos estratégicos de TI en una iniciativa acordada y aprobada.

- **11 Optimización de activos, recursos y capacidades de las TI :**

1. Frecuencia de evaluaciones de la madurez de la capacidad y de la optimización de costes.
2. Tendencia de los resultados de las evaluaciones.
3. Niveles de satisfacción del Fiscal General de la Nación y TI con los costes y capacidades TI.

Objetivos y Métricas de Procesos

1. La arquitectura y los estándares son eficaces apoyando a la empresa.

1. Número de excepciones solicitadas y concedidas en los estándares de la arquitectura básica.
2. Nivel de realimentación sobre la arquitectura por parte del cliente.
3. Beneficios aportados por el proyecto que pueden ser trazados a la implicación de la arquitectura (por ejemplo, reducción de costes debido a la reutilización).

2. La cartera de servicios de la arquitectura de empresa soporta el cambio empresarial ágil.

1. Porcentaje de proyectos que usan los servicios de la arquitectura de la entidad.
2. Nivel de retroalimentación sobre la arquitectura por parte del cliente.

3. Existen dominios apropiados y actualizados y/o arquitecturas federadas que proveen información fiable de la arquitectura.

1. Fecha de la última actualización en el dominio y/o arquitecturas federadas.
2. Número de deficiencias detectadas en los modelos a lo largo de los dominios de la entidad, estrategia de TI, gobierno de TI, información, sistemas de información, servicios tecnológicos, uso y apropiación.
3. Nivel de realimentación del cliente de la arquitectura en relación a la calidad de la información proporcionada

4. Se utiliza un marco de arquitectura de empresa y una metodología común, así como un repositorio de arquitectura integrado, con el fin de permitir la reutilización de eficiencias dentro de la empresa.

1. Porcentaje de proyectos que utilizan el marco de trabajo y la metodología para reutilizar componentes ya definidos.

2. Número de personas formadas en la metodología y en el manejo del conjunto de herramientas.

Número de excepciones concedidas en los estándares de la arquitectura básica. Aplicando la matriz RACI para la entidad se obtiene:

MATRIZ RACI APO03- APLICADO A LA ENTIDAD (F.G.N.)

MATRIZ RACI APO03 - FISCALIA GENERAL DE LA NACION																												
PRACTICA CLAVE DE GOBIERNO	PRESIDENTE COLOMBIA	FISCAL GENERAL DE LA NACION (CEO)	VICEFISCAL (CFO)	DIRECTOR NACIONAL DE APOYO A LA GESTION (COO)	SUBDIRECCION FINANCIERA	LIDERES DE LOS PROCESOS (DIRECTORES OFICINAS)	DIRECCION NACIONAL DE POLITICAS PUBLICAS Y DE PLANEACION	DIRECCION NACIONAL DE ESTRATEGIAS CONSTITUCIONALES	GESTOR DE PROYECTOS	OFICINA GESTIÓN DEL VALOR	DIRECTOR DE RIESGOS (CRO)	DIRECTOR DE SEGURIDAD DE LA INFORMACIÓN (CISO)	DIRECTOR DE ARQUITECTURA EMPRESARIAL	COMITÉ DE RIESGOS CORPORATIVOS	JEFE DE TALENTO HUMANO	DIRECCIÓN JURIDICA (COMPILANCE)	DIRECCIÓN DE CONTROL INTERNO	SUBDIRECTOR DE LAS TICs (CIO)	JEFE ARQUITECTURA DE NEGOCIO	JEFE DPTO INFRAESTRUCTURA TECNOLOGICA	JEFE DPTO SISTEMAS DE INFORMACIÓN	JEFE DE COMUNICACIONES	JEFE DE SEGURIDAD	ASESOR DE PROCESOS Y ASEGURAMIENTO DE LA CALIDAD	JEFE ATENCIÓN REQUERIMIENTOS INFORMATICOS Y	JEFE CONTINUIDAD DE NEGOCIO
APO03.01 - Desarollar la visión de la arquitectura de la Fiscalía General de la Nación		A	C	C	R	C	R					C	R	C	C	C	C	R	R	C	C	C		C		
APO03.02 Definir la arquitectura de referencia establecida para las entidades del estado		C	C	C	R	C	R					C	A	C	C	C	C	R	R	C	C	C		C		
APO03.03 Seleccionar las oportunidades y soluciones		A	C	C	R	C	R					C	R	C	C	C	C	R	R	C	C	C		C		
APO03.04 Definir la implantación de la arquitectura		A	C	R	C	C	R					C	R	C	C	C	C	R	R	C	C	C		C		
APO03.05 Proveer los servicios de AE		A	C	R	C	C	R					C	R	C	C	C	C	R	R	C	C	C		C		

FIG. 25 Matriz RACI – FGN – APO03

Fuente: Iniciativa Propia

	ESTADO ACTUAL -AS IS
	ESTADO DESEADO - TO BE

APO03-01 Prácticas, Entradas/Salidas y Actividades del Proceso

La visión de la arquitectura proporciona una primera descripción de alto nivel de las arquitecturas de partida y objetivo, cubriendo los dominios de la Fiscalía General de la Nación, estrategia de TI, gobierno de TI, información, sistemas de información, servicios tecnológicos, uso y apropiación, dominios del modelo de arquitectura empresarial establecido por el estado colombiano. La visión de la arquitectura proporciona al promotor la herramienta clave para entregar los beneficios de la capacidad propuesta a los usuarios de la administración de justicia. La visión de la arquitectura de información describe como nuevas capacidades y permitirá alcanzar las metas de la entidad y los objetivos estratégicos y considerara las preocupaciones e intereses de las partes interesadas en su implementación.

Entradas:

1- Principios, directrices de la arquitectura de la Fiscalía General de la Nación.
2- Hoja de ruta de la estrategia.
3- Estrategia empresarial (institucional).

Salidas:

1- Alcance de la arquitectura definido
2- Principios de la arquitectura
3- Caso de negocio y propuesta de valor del concepto de arquitectura.

APO03.01 Actividades:

1- Identificar a las partes interesadas clave de la F.G.N. y sus objetivos/preocupaciones y definir los requisitos clave a ser considerados, así como la visión de la arquitectura a ser desarrollada para satisfacer los distintos requisitos de las partes interesadas.

2- Identificar los objetivos y los impulsores estratégicos de la F.G.N y definir las limitaciones con las que habrá que tratar, incluyendo las limitaciones en toda la entidad y las específicas del proyecto (duración, planificación, recursos, etc.).

3- Alinear los objetivos de la arquitectura con las prioridades estratégicas del plan empresarial (institucional).

4- Entender los deseos y las capacidades de la F.G.N y, a continuación, identificar las opciones para realizar dichas capacidades.

5- Evaluar la disposición de la entidad para el cambio.

6- Definir qué está dentro y qué está fuera del alcance de la arquitectura de partida y los esfuerzos de arquitectura objetivo, entendiendo que el punto de partida y el objetivo no necesitan ser descritos con el mismo nivel de detalle.

7- Confirmar y elaborar los principios de la arquitectura, incluyéndose los principios de la empresa. Asegurarse de que todas las definiciones existentes están vigentes y aclarar cualquier área de ambigüedad.

8- Entender los objetivos estratégicos actuales de la entidad y trabajar conjuntamente con los procesos de planificación estratégica para asegurarse que las oportunidades de arquitectura de TI empresarial se apoyan en el desarrollo del plan estratégico.

9- Crear la visión de la arquitectura atendiendo a las preocupaciones de las partes interesadas, en los requisitos de capacidad de la entidad, en el

alcance, en las limitaciones y principios: visión de alto nivel de las arquitecturas de partida y objetivo.

10- Definir las proposiciones de valor, los objetivos y métricas de la arquitectura objetivo.

11- Identificar los riesgos institucionales asociados con el cambio de la nueva visión de la arquitectura, evaluar el nivel de riesgo inicial (por ejemplo, crítico, marginal o despreciable) y desarrollar una estrategia de mitigación para cada riesgo importante.

12- Desarrollar el caso de negocio del concepto de arquitectura empresarial, bosquejar los planes y el trabajo de arquitectura y asegurar que están aprobados para iniciar el proyecto que esté alineado e integrado con la estrategia empresarial (institucional).

APO03-02 Prácticas, Entradas/Salidas y Actividades del Proceso

Definir la arquitectura de referencia. La arquitectura de referencia tomada para la Fiscalía General de la Nación, es la establecida por el gobierno colombiano, donde se describe la situación actual y el objetivo de la arquitectura para los dominios Estrategia de TI, Gobierno de TI, Información, Sistemas de Información, Servicios Tecnológicos, Uso y Apropiación.

Entradas:

1- Directrices operativas corporativas (directrices misionales), definición de la estructura de la entidad y sus funciones.

2- Emplazamiento operacional de la función TI, evaluación de las diferentes opciones para la organización de TI.

3- Guía para la clasificación de los datos.

4- Estrategia empresarial (institucional).

Salidas:

1- Descripción del dominio de partida y definición de la arquitectura.

2- Modelo de arquitectura de procesos.

3- Modelo de la arquitectura de información (datos, activos de información más valiosos para la Fiscalía)

APO03.02 Actividades:

1- Mantener un repositorio de la arquitectura que contenga los estándares, los componentes reutilizables, el modelado, las relaciones, las dependencias y las vistas para permitir una uniformidad en la entidad y el mantenimiento.

2- Seleccionar los puntos de vista de referencia del repositorio de arquitectura que permitirán al arquitecto demostrar cómo están siendo consideradas las preocupaciones de las partes interesadas en la arquitectura.

3- Por cada punto de vista, seleccionar los modelos necesarios para soportar cada uno de ellos, utilizando las herramientas o métodos seleccionados y los niveles apropiados de descomposición.

4- Desarrollar descripciones de dominio de arquitectura de partida, utilizando el alcance y nivel de detalle necesario para apoyar la arquitectura objetivo y, hasta el punto que sea posible, identificando los bloques relevantes del repositorio de la arquitectura.

5- Mantener un modelo de arquitectura de procesos como parte de las descripciones de dominio de referencia y objetivo. Estandarizar las descripciones y la documentación de los procesos. Definir las funciones y responsabilidades de los que deciden el proceso, el propietario del proceso, los usuarios del proceso, el equipo del proceso y cualquier otra parte interesada que debieran estar involucrados.

6- Mantener un modelo de arquitectura de información como parte de las descripciones de dominio de referencia y objetivo, que sea consistente con la estrategia de la entidad y que permita un uso óptimo de la información para la toma de decisiones. Mantener un diccionario de datos de la entidad que promueva una interpretación común y un esquema de clasificación que incluya detalles sobre el propietario de los datos, definición de los niveles de seguridad apropiados y los requisitos de retención y destrucción de los datos.

7- Verificar la consistencia interna y precisión de los modelos de la arquitectura y realizar un análisis de diferencias entre el punto de partida y el objetivo. Priorizar las desviaciones y definir los nuevos componentes o modificaciones que se deben desarrollar en la arquitectura objetivo. Resolver los impactos potenciales, tales como las incompatibilidades, inconsistencias o conflictos dentro de la arquitectura prevista.

8- Realizar una revisión formal con las partes interesadas para comprobar que la arquitectura propuesta frente a la motivación original del proyecto de arquitectura y la declaración de arquitectura funcionan.

9- Finalizar la arquitectura de los dominios de negocio, información, datos, aplicaciones y tecnología y crear un documento de definición de la arquitectura.

APO03-03 Prácticas, Entradas/Salidas y Actividades del Proceso

Seleccionar las oportunidades y las soluciones. Racionalizar las desviaciones entre las arquitecturas de referencia y objetivo, considerando tanto la perspectiva técnica como la del negocio y agrupándolos a ambos en paquetes de trabajo del proyecto. Integrar el proyecto con todos los programas de inversión relacionados con TI, para asegurar que las iniciativas relacionadas con la arquitectura estén alineadas y que estas iniciativas sean parte del cambio general en la entidad. Hacer de ello un esfuerzo en colaboración con las partes interesadas clave de la entidad y en TI para evaluar el grado de preparación de la entidad para su transformación e identificar las oportunidades, soluciones y todas las restricciones de la implementación.

Entradas:

1- Cambios propuestos en la arquitectura de la entidad.

2- Estrategias empresariales (institucionales) y motivadores de la entidad.

Salidas:

1- Estrategia de Implementación a alto nivel y estrategia de migración.

2- Arquitectura de transición.

APO03.03 Actividades:

1- Determinar y confirmar los atributos clave del cambio, incluyendo la cultura institucional y cómo ésta impactará en la implementación de la arquitectura de la entidad, así como en las capacidades de transición institucional.

2- Identificar los motivadores de la fiscalía que podrían limitar la secuencia de implementación, incluyendo una revisión de los planes estratégicos y de negocio de la entidad y de las líneas de negocio y considerando la madurez de la arquitectura de FGN actual[6].

3- Revisar y consolidar los resultados del análisis de diferencias entre las arquitecturas de partida y objetivo y evaluar sus implicaciones respecto a las potenciales oportunidades y soluciones, interdependencias y alineación con los vigentes programas habilitados para TI.

4- Evaluar las necesidades, las carencias, las soluciones y los factores para identificar un conjunto mínimo de requisitos funcionales cuya integración en el plan de trabajo daría lugar a una implementación más eficiente y eficaz de la arquitectura objetivo.

[6] Los cambios de fiscal cada 4 años hace que se cambie en forma o en fondo el direccionamiento estratégico, con efecto en el ajuste de los objetivos de la entidad

5- Conciliar los requisitos ya consolidados con las posibles soluciones.

6- Afinar las dependencias iniciales, asegurándose que todas las restricciones sobre los planes de implementación y migración están identificadas y se han consolidado en el informe de análisis de dependencias.

7- Confirmar el grado de preparación de la Fiscalía y el riesgo asociado a la transformación institucional.[7]

8- Formular una implementación de alto nivel y una estrategia de migración que servirán de guía para la implementación de la arquitectura objetivo y para la estructura de la arquitectura de transición en línea con los objetivos estratégicos y los plazos de la entidad.

9- Identificar y agrupar los principales paquetes de trabajo en un conjunto de programas y proyectos coherentes, respetando el enfoque y la dirección de la estrategia institucional en su implementación.

10- Desarrollar una serie de arquitecturas de transición cuando sea necesario un enfoque incremental por el alcance del cambio necesario para alcanzar la arquitectura de información objetivo.

APO03-04 Prácticas, Entradas/Salidas y Actividades del Proceso

Definir la implementación de la arquitectura. Crear un plan de implementación y de migración viable acorde con la cartera de proyectos y programas. Asegurarse

[7] Actualmente en la FGN no se han presentado proyectos de AE por parte de la subdirección de TICS, para la asignación de presupuesto.

que el plan está coordinado de cerca para asegurar que se proporciona el valor y que se disponen de los recursos necesarios para finalizar los trabajos.

Entradas:

No se tienen entradas para esta guía práctica.

Salidas:

1- Necesidades de recursos.

2- Descripciones de las fases de implementación.

3- Requisitos de gobierno de la arquitectura.

APO03.04 Actividades:

1- Establecer lo que el plan de implementación y migración deberían incluir como parte del programa y plan de proyectos para asegurarse que están alineados con los requisitos de los decisores aplicables.

2- Confirmar las fases y los progresos de la arquitectura de transición y actualizarlos en el documento de definición de la arquitectura.
3- Definir los requisitos de gobierno de implementación de la arquitectura.

APO03-05 Prácticas, Entradas/Salidas y Actividades del Proceso

Proveer los servicios de arquitectura empresarial. La provisión de los servicios de arquitectura empresarial incluye las guías y supervisión de los proyectos a implementar, la formalización de las maneras de trabajar mediante los contratos de

arquitectura, la medición y comunicación de los valores aportados por la arquitectura y la supervisión del cumplimiento.

Entradas:

No se tienen entradas para esta guía práctica

Salidas:

1- Orientación para el desarrollo de soluciones

APO03.05 Actividades:

1- Confirmar el alcance y las prioridades y proporcionar orientación para el desarrollo y despliegue de soluciones.

2- Gestionar la cartera de servicios de arquitectura de la entidad para asegurar el alineamiento con los objetivos estratégicos y el desarrollo de soluciones.

3- Gestionar los requisitos de la arquitectura empresarial y dar soporte con los principios de dicha arquitectura, modelos y componentes básicos.

4- Identificar y alinear las prioridades de la arquitectura empresarial a los motivadores del valor. Definir y recoger los valores de las medidas y las métricas utilizadas y comunicar el valor de la arquitectura empresarial.
5- Establecer un foro tecnológico para facilitar guías de uso de la arquitectura, soporte en los proyectos y guía en la selección de la tecnología. Medir el cumplimiento con estos estándares y guías de referencia, incluyendo el cumplimiento con requisitos externos y su importancia para el negocio.

Línea de Madurez APO03 – Entidad (FGN)

Alinear, Planificar y Organizar

APO03- Establecer una AE en la F.G.N	NIVEL ACTUAL	NIVEL ESPERADO
APO03.01 - Desarrollar la visión de la arquitectura de la Fiscalía General de la Nación	0	2
APO03.02 Definir la arquitectura de referencia establecida para las entidades del estado	1	3
APO03.03 Seleccionar las oportunidades y soluciones	0	3
APO03.04 Definir la implantación de la arquitectura	0	3
APO03.05 Proveer los servicios de AE	0	3

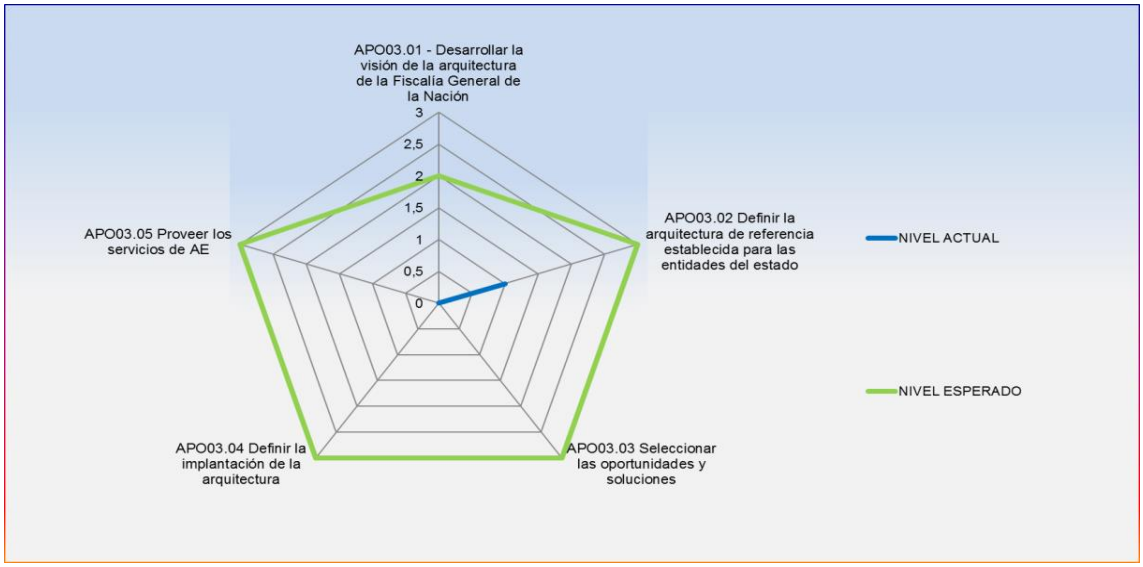


Figura 26: Modelo Madurez APO03-FGN

Fuente: Iniciativa propia

APO12: Gestionar el Riesgo en la entidad (F.G.N) alinear, planificar y organizar

Descripción del Proceso

Identificar, evaluar y reducir los riesgos relacionados con TI de forma continua, dentro de niveles de tolerancia establecidos por el Fiscal General de la Nación.

Declaración del Propósito del Proceso

Integrar la gestión de riesgos institucionales relacionados con TI con la gestión de riesgos institucionales generales y equilibrar los costes y beneficios de gestionar riesgos institucionales relacionados con TI.

Metas de TI con sus respectivas Métricas Relacionadas

Objetivos y Métricas de Procesos

- **02 Cumplimiento y soporte de las TI** al cumplimiento del negocio de las leyes y regulaciones externas

1. Coste del incumplimiento de TI, incluyendo acuerdos judiciales y multas, y el impacto de pérdida de reputación.

2. Número de asuntos de incumplimiento relacionados con TI reportados a la junta que llegan a ser de dominio público o que provocan situaciones de escándalo.

3. Número de asuntos de incumplimiento relacionados con acuerdos contractuales con proveedores de servicio TI.

4. Cobertura de la evaluación del cumplimiento.

- **04 Riesgos de negocio relacionados con las TI gestionados**

1. Porcentaje de procesos institucionales críticos, servicios TI y programas de negocio habilitados por las TI cubiertos por evaluaciones de riesgos.

2. Número de incidentes significativos relacionados con las TI que no fueron identificados en la evaluación de riesgos.

3. Porcentaje de evaluaciones de riesgo de la entidad que incluyen los riesgos relacionados con TI.

4. Frecuencia de actualización del perfil de riesgo.

- **06 Transparencia de los costes, beneficios y riesgo de las TI**

1. Porcentaje de inversión en casos de negocio con costes y beneficios esperados relativos a TI claramente definidos y aprobados.

2. Porcentaje de servicios TI con costes operativos y beneficios esperados claramente definidos y aprobados.

3. Encuesta de satisfacción a las partes interesadas clave relativa al nivel de transparencia, comprensión y precisión de la información financiera de TI.

- **10 Seguridad de la información, infraestructura de procesamiento y aplicaciones**

1. Número de incidentes de seguridad causantes de pérdidas financieras, interrupciones del negocio o pérdida de imagen pública.

2. Número de servicios de TI con los requisitos de seguridad pendientes.

3. Tiempo para otorgar, modificar y eliminar los privilegios de acceso, comparado con los niveles de servicio acordados.

4. Frecuencia de la evaluación de seguridad frente a los últimos estándares y guías (Primera evaluación aprobada y realizada del 18 al 28 de octubre de 2016 por la dirección de control interno).

- **13 Entrega de programas que proporcionen beneficios a tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas de calidad**

1. Número de programas/proyectos ejecutados en plazo y en presupuesto.

2. Porcentaje de partes interesadas satisfechas con la calidad del programa/proyecto.

3. Número de programas que necesitan ser revisados significativamente debido a defectos de calidad.

4. Coste del mantenimiento de aplicaciones respecto al coste total de TI.

Objetivos y Métricas de Procesos

El riesgo relacionado con TI está identificado, analizado, gestionado y reportado.

1. Grado de visibilidad y reconocimiento en el entorno actual.

2. Número de eventos de pérdida con características clave, capturados en repositorios.

3. Porcentaje de auditorías, eventos y tendencias capturados en repositorios.

2. Existe un perfil de riesgo actual y completo.

1. Porcentaje de procesos de negocio claves incluidos en el perfil de riesgo.

2. Completitud de atributos y valores en el perfil de riesgo

3. Todas las acciones de gestión para los riesgos significativos están gestionadas y bajo control.

    1. Porcentaje de propuestas de gestión de riesgos rechazadas debido a una falta de consideración sobre algún riesgo relacionado.

    2. Número de incidentes significativos no identificados e incluidos en el portafolio de gestión de riesgos.

4. **Las acciones de gestión de riesgos están efectivamente implementadas.**

    1. Porcentaje de planes de acción para riesgos de TI ejecutados de la forma que fueron diseñados.

    2. Número de medidas que no reducen el riesgo residual.

MATRIZ RACI APO12- APLICADO A LA ENTIDADA (FGN)

MATRIZ RACI APO03 - FISCALIA GENERAL DE LA NACION																										
PRACTICA CLAVE DE GOBIERNO	PRESIDENTE COLOMBIA	FISCAL GENERAL DE LA NACION (CEO)	VICEFISCAL (CFO)	DIRECTOR NACIONAL DE APOYO A LA GESTION (COO)	SUBDIRECCION FINANCIERA	LIDERES DE LOS PROCESOS (DIRECTORES OFICINAS)	DIRECCION NACIONAL DE POLITICAS PUBLICAS Y DE PLANEACION	DIRECCION NACIONAL DE ESTRATEGIAS CONSTITUCIONALES	GESTOR DE PROYECTOS	OFICINA GESTIÓN DEL VALOR	DIRECTOR DE RIESGOS (CRO)	DIRECTOR DE SEGURIDAD DE LA INFORMACIÓN (CISO)	DIRECTOR DE ARQUITECTURA EMPRESARIAL	COMITÉ DE RIESGOS CORPORATIVOS	JEFE DE TALENTO HUMANO	DIRECCIÓN JURIDICA (COMPILANCE)	DIRECCIÓN DE CONTROL INTERNO	SUBDIRECTOR DE LAS TICs (CIO)	JEFE ARQUITECTURA DE NEGOCIO	JEFE DPTO INFRAESTRUCTURA TECNOLOGICA	JEFE DPTO SISTEMAS DE INFORMACIÓN	JEFE DE COMUNICACIONES	JEFE DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION	ASESOR DE PROCESOS Y ASEGURAMIENTO DE LA CALIDAD	JEFE ATENCIÓN REQUERIMIENTOS INFORMATICOS Y	JEFE CONTINUIDAD DE NEGOCIO
APO12.01 Recopilar datos		I				R			R		R	R		I		C	C	A	R	R	R	R	R	R	R	R
APO12.02 Analizar el riesgo		I				R			C		R	C		I		R	R	A	C	C	C	C	C	C	C	C
APO12.03 Mnatener un perfil de riesgo		I				R			C		A	C		I		R	R	R	C	C	C	C	C	C	C	C
APO12.04 Expresar el riesgo		I				R			C		R	C		I		C	C	A	C	C	C	C	C	C	C	C
APO12.05 Definir un portafolio de acciones para la gestion de riesgos		I				R			C		A	C		I		C	C	R	C	C	C	C	C	C	C	C
APO12.06 Responder al riesgo		I				R			R		R	R		I		C	C	A	R	R	R	R	R	R	R	R

Figura 27: Matriz RACI - APO12-FGN

Fuente: Iniciativa propia

	ESTADO ACTUAL -AS IS
	ESTADO DESEADO - TO BE

APO12-01 Prácticas, Entradas/Salidas y Actividades del Proceso

Recopilar datos: Identificar y recopilar datos relevantes para catalizar una identificación, análisis y notificación efectiva de riesgos relacionados con TI.

Entradas:

1- Evaluación de actividades de gestión de riesgos.

2- Procesos aprobados, para medir la gestión de riesgos. Objetivos clave a ser monitorizados por la gestión de riesgos. Políticas de gestión de riesgos.

3- Brechas y riesgos relacionados con capacidades actuales.

4- Evaluación del riesgo.

5- Riesgo de entrega de proveedores identificados.

6- Estado de incidentes e informe de tendencias.

Salidas:

1- Datos en el entorno de operación relacionados con el riesgo.

2- Datos en eventos de riesgo y en factores contribuyentes.

3- Elementos y factores de riesgo emergentes

APO12.01 - Actividades:

1. Establecer y mantener un método para la recogida, clasificación y análisis de datos relacionados con riesgo de TI, dando cabida a múltiples tipos de

eventos, múltiples categorías de riesgo de TI y múltiples factores de riesgo (en la entidad no se realiza de esta forma solo se tienen en el mapa de riesgos institucional un riesgo de gestión y un riesgo de corrupción).

2. Registrar datos relevantes sobre el entorno de operación interno y externo de la entidad que pudieran jugar un papel significativo en la gestión del riesgo de TI.

3. Medir y analizar los datos históricos de riesgo de TI y de pérdidas experimentadas tomados de datos y tendencias externas disponibles, entidades del estado similares – basados en eventos registrados, bases de datos y acuerdos de la industria sobre divulgación de eventos comunes.

4. Registrar datos sobre eventos de riesgo que han causado o pueden causar impactos al beneficio/valor facilitado por TI, a la entrega de programas y proyectos de TI y/o a las operaciones y entrega de servicio de TI. Capturar datos relevantes sobre asuntos relacionados, incidentes, problemas e investigaciones.

5. Para clases o eventos similares, organizar los datos recogidos y destacar factores contribuyentes. Determinar los factores contribuyentes comunes para eventos múltiples.

6. Determinar las condiciones específicas que existían o faltaban cuando ocurrieron los eventos de riesgo y la forma en la cual las condiciones afectaban la frecuencia del evento y la magnitud de la pérdida.

7. Ejecutar análisis periódicos de eventos y de factores de riesgo para identificar asuntos nuevos o emergentes relacionados con el riesgo y para obtener un entendimiento de los asociados factores de riesgo internos y externos.

APO12-02 Prácticas, Entradas/Salidas y Actividades del Proceso

Analizar el riesgo. Desarrollar información útil para soportar las decisiones relacionadas con el riesgo que tomen en cuenta la relevancia para el negocio de los factores de riesgo.

Entradas:

1- Análisis de impacto en la entidad.

2- Evaluaciones de amenazas potenciales.

3- Avisos de amenaza

Salidas:

1- Alcance de los esfuerzos de análisis de riesgos.

2- Escenarios de riesgo de TI.

3- Resultados de análisis de riesgos.

APO12.02 - Actividades:

1- Definir la amplitud y profundidad apropiada para los esfuerzos en análisis de riesgos, considerando todos los factores de riesgo y la criticidad en la entidad

de los activos. Establecer el alcance del análisis de riesgos después de llevar a cabo un análisis coste-beneficio.

2- Construir y actualizar regularmente escenarios de riesgo de TI, que incluyan escenarios compuestos en cascada y/o tipos de amenaza coincidentes y desarrollar expectativas para actividades de control específicas, capacidades para detectar y otras medidas de respuesta.

3- Estimar la frecuencia y magnitud de pérdida o ganancia asociada con escenarios de riesgo de TI. Tener en cuenta todos los factores de riesgo que apliquen, evaluar controles operacionales conocidos y estimar niveles de riesgo residual.

4- Comparar el riesgo residual con la tolerancia al riesgo e identificar exposiciones que puedan requerir una respuesta al riesgo.

5- Analizar el coste-beneficio de las opciones de respuesta al riesgo potencial, tales como evitar, reducir/mitigar, transferir/compartir y aceptar y explotar/capturar. Proponer la respuesta al riesgo óptima.

6- Especificar requerimientos de alto nivel para los proyectos o programas que implementarán las respuestas de riesgo seleccionadas. Identificar requerimientos y expectativas para los controles clave que son apropiados para las respuestas de mitigación de riesgos.

7- Validar los resultados de análisis de riesgos antes de usarlos para la toma de decisiones, confirmando que los análisis se alinean con requerimientos de la entidad y verificando que las estimaciones fueron apropiadamente calibradas y examinadas ante una posible parcialidad.

APO12-03 Prácticas, Entradas/Salidas y Actividades del Proceso

Mantener un perfil de riesgo: Mantener un inventario del riesgo conocido y atributos de riesgo (incluyendo frecuencia esperada, impacto potencial y respuestas) y de otros recursos, capacidades y actividades de control actuales relacionados.

Entradas:

1- Niveles aprobados de tolerancia al riesgo. Guía de apetito al riesgo.

2- Riesgo de entrega de proveedores identificados.

3- Evaluaciones de amenazas potenciales.

Salidas:

1- Escenarios de riesgo documentados por procesos implementados en la entidad y de acuerdo con su función.

2- Perfil de riesgo agregado, incluyendo el estado de las acciones de gestión del riesgo.

APO12.03 - Actividades:

1- Inventariar los procesos de negocio, incluyendo el personal de soporte, aplicaciones, infraestructura, instalaciones, registros manuales críticos, proveedores y externalizados y documentar la dependencia de los procesos de gestión de servicio TI y de los recursos de infraestructuras TI.

2- Determinar y acordar qué servicios TI y recursos de infraestructuras de TI son esenciales para sostener la operación de procesos de negocio. Analizar dependencias e identificar eslabones débiles.

3- Agregar escenarios de riesgo actuales, por categoría, línea de negocio y área funcional.

4- De forma regular, capturar toda la información sobre el perfil de riesgo y consolidarla dentro de un perfil de riesgo agregado.

5- Sobre la base de todos los datos del perfil de riesgo, definir un conjunto de indicadores de riesgo que permitan la identificación rápida y la supervisión del riesgo actual y las tendencias de riesgo.

6- Capturar información sobre eventos de riesgos de TI que se han materializado, para su inclusión en el perfil de riesgo de TI de la entidad.

7- Capturar información sobre el estado del plan de acción del riesgo, para la inclusión en el perfil de riesgo de TI de la entidad.

APO12-04 Prácticas, Entradas/Salidas y Actividades del Proceso

Expresar el riesgo: Proporcionar información sobre el estado actual de exposiciones y oportunidades relacionadas con TI de una forma oportuna a todas las partes interesadas necesarias para una respuesta apropiada.

Entradas:

- No se tienen entradas para esta guía práctica.

Salidas:

1- Análisis de riesgos e informes del perfil de riesgos para las partes interesadas.

2- Revisión de resultados de evaluaciones de riesgos de terceras partes.

3- Oportunidades para la aceptación de un riesgo mayor.

APO12.04 - Actividades:

1- Informar de los resultados del análisis de riesgos a todas las partes interesadas afectadas en términos y formatos útiles para soportar las decisiones de la entidad. Cuando sea posible, incluir probabilidades y rangos de pérdida o ganancia junto con niveles de confianza que permitan a la dirección equilibrar el retorno del riesgo.

2- Proporcionar a los responsables de toma de decisiones un entendimiento de los escenarios peor y más probables, exposiciones de diligencia debida y consideraciones sobre la reputación, legales y regulatorias significativas.

3- Informar el perfil de riesgo actual a todas las partes interesadas, incluyendo la efectividad del proceso de gestión de riesgos, la efectividad de los controles, diferencias, inconsistencias, redundancias, estado de la remediación y sus impactos en el perfil de riesgo.

4- Revisar los resultados de evaluaciones objetivas de terceras partes, auditorías internas y revisiones del aseguramiento de la calidad y mapearlos con el perfil de riesgo. Revisar las diferencias y exposiciones identificadas para determinar la necesidad de análisis de riesgos adicionales.

5- De forma periódica, para áreas con un riesgo relativo y una paridad de capacidad del riesgo, identificar oportunidades relacionadas con TI que podría permitir la aceptación de un mayor riesgo y un crecimiento y retorno mayores.

APO12-05 Prácticas, Entradas/Salidas y Actividades del Proceso

Definir un portafolio de acciones para la gestión de riesgos: Gestionar las oportunidades para reducir el riesgo a un nivel aceptable como un portafolio.

Entradas:

- No se tienen entradas para esta guía práctica

Salidas:

1- Propuestas de proyecto para reducir el riesgo

APO12.05 - Actividades:

1- Mantener un inventario de actividades de control que estén en marcha para gestionar al riesgo y que permitan que el riesgo que se tome esté alineado con el apetito y tolerancia al riesgo. Clasificar las actividades de control y mapearlas con las declaraciones de riesgo específicas de TI y agrupaciones de riesgo de TI.

2- Determinar si cada proceso de la entidad supervisa el riesgo y acepta la responsabilidad para operar dentro de sus niveles de tolerancia individuales y de portafolio.

3- Definir un conjunto de propuestas de proyecto equilibradas diseñadas para reducir el riesgo y/o proyectos que permitan oportunidades estratégicas institucionales, considerando costes/beneficios, el efecto en el perfil de riesgo actual y las regulaciones.

APO12-06 Prácticas, Entradas/Salidas y Actividades del Proceso

Responder al riesgo: Responder de una forma oportuna con medidas efectivas que limiten la magnitud de pérdida por eventos relacionados con TI.

Entradas:

1- Acciones correctoras para tratar las desviaciones de gestión de riesgos.

Salidas:

1- Planes de respuesta para incidentes relacionados con el riesgo.

2- Comunicaciones del impacto del riesgo.

3- Causas raíz relacionadas con el riesgo

APO12.06 - Actividades:

1- Preparar, mantener y probar planes que documenten los pasos específicos a tomar cuando un evento de riesgo pueda causar un incidente significativo operativo o evolucionar en un incidente con un impacto de negocio grave. Asegurar que los planes incluyan vías de escalado a través de la entidad.

2- Categorizar los incidentes y comparar las exposiciones reales con los umbrales de tolerancia al riesgo. Comunicar los impactos en la entidad a los

responsables de la toma de decisiones como parte de la notificación y actualizar el perfil de riesgo.

3- Aplicar el plan de respuesta apropiado para minimizar el impacto cuando ocurren incidentes de riesgo.

4- Examinar eventos adversos/pérdidas del pasado y oportunidades perdidas y determinar sus causas raíz. Comunicar la causa raíz, requerimientos de respuesta adicionales para el riesgo y mejoras de proceso a los responsables de toma de decisiones apropiados y asegurarse de que la causa, los requerimientos de respuesta y la mejora del proceso se incluyan en los procesos de gobierno del riesgo.

Aplicando Línea de Madurez al proceso seleccionado:

Alinear, Planificar y Organizar

APO12- Gestionar el Riesgo en la F.G.N	NIVEL ACTUAL	NIVEL ESPERADO
APO12.01 Recopilar datos.	2	3
APO12.02 Analizar el riesgo.	2	3
APO12.03 Mantener un perfil de riesgo.	2	3
APO12.04 Expresar el riesgo.	2	3
APO12.05 Definir un portafolio de acciones para la gestión de riesgos.	1	3
APO12.06 Responder al riesgo.	1	3

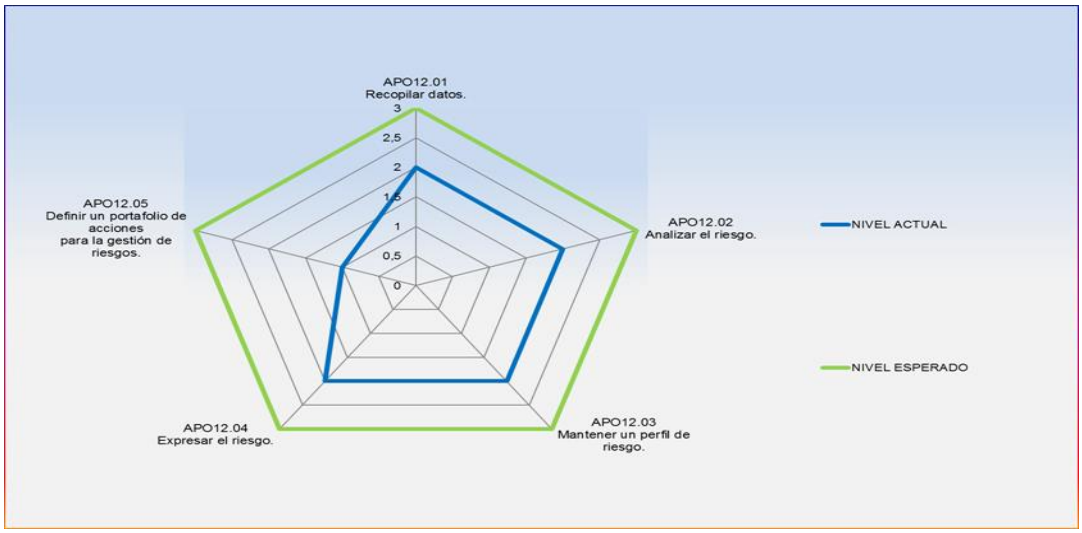


Figura 28: Línea de Madurez APO12-FGN

Fuente: Iniciativa propia

5.3. Fase III. Construcción:

Diseñar y documentar la guía propuesta a partir del resultado de la fase 2. La guía constará de una serie de sub fases para las que se especificarán las entradas y salidas de cada una, así como las actividades a realizar dentro de ellas, aplicando los productos de la fase 2.

Esta guía de implementación establece una propuesta de alternativas que constituyen evidencias que debe obtener la una entidad de control, para este caso se tomó como modelo para la F.G.N, como cumplimiento al Marco de Referencia de AE para la gestión de TI del estado Colombiano. Teniendo en cuenta, además, que se integra como propuesta la gestión de riesgos transversales a todos los procesos que interactúan con el área de TI de la entidad. (En las subfases se subrayan algunos textos para acentuar que es algo adicional o de valor agregado a lo existente y de eso se alcanzaron a implementar y/o poner en práctica en el proyecto con todo lo evidenciado en el trabajo de campo)

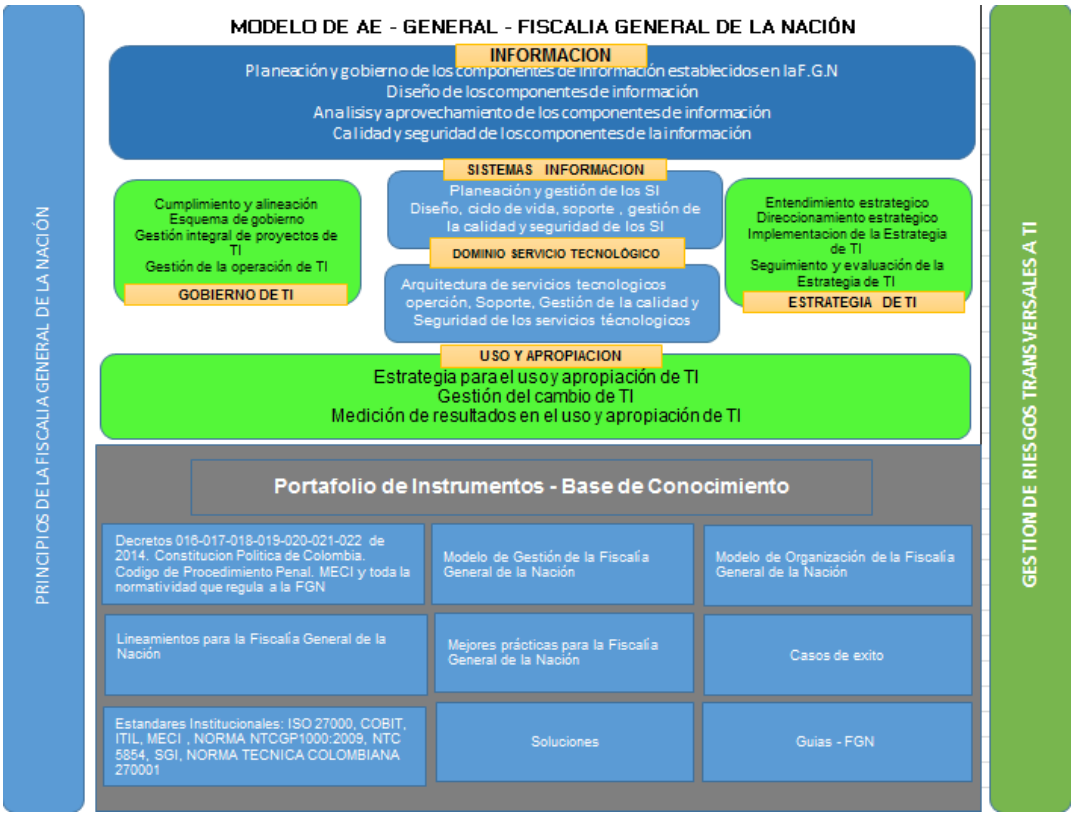


Figura 29: Modelo de AE – General para una entidad de control

Fuente: Iniciativa propia y resultado de este trabajo de grado (Complementa la implementación de AE en la FGN) y tomando como base el modelo de AE propuesto por MINTIC

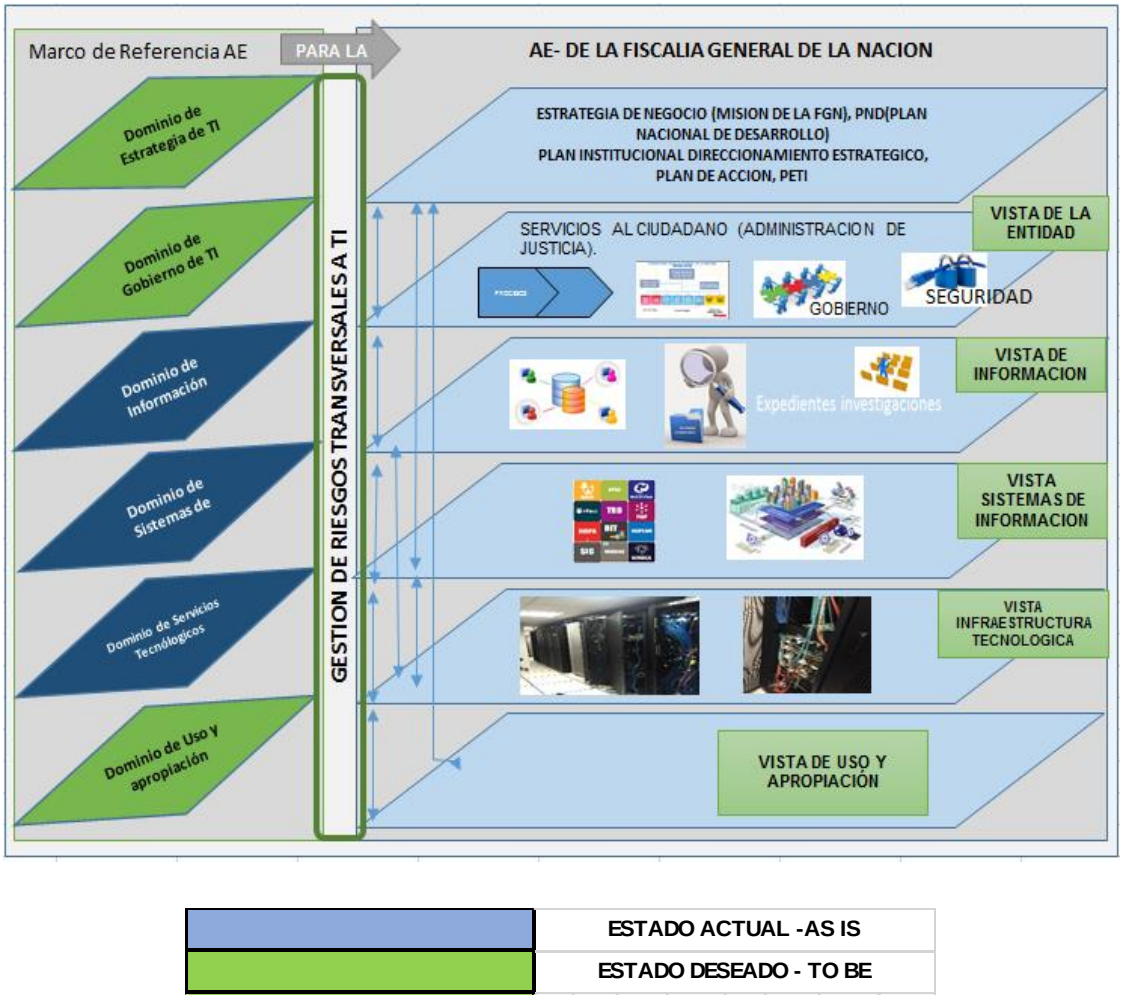


Figura 30: Modelo de AE – Diseño Detallado para una entidad de control

Fuente: Iniciativa propia tomando como base el modelo de AE de MINTIC

A continuación se presentan las salidas de cada uno de los lineamientos del Marco de Referencia de AE para la gestión de TI en el estado Colombiano. Estas salidas se agrupan por ámbitos dentro de cada uno de los dominios establecidos:

Dominios del Marco de referencia de AE:

- Estrategia de TI
- Gobierno de TI
- Información

- Sistemas de Información
- Servicios Tecnológicos
- Uso y apropiación

Dominio transversal no incluido dentro del Marco de referencia de AE:

- Gestión de riesgos transversales a TI

5.3.1 DOMINIO ESTRATEGIA DE TI – APLICADO A LA ENTIDAD DE CONTROL (F.G.N)

Este dominio tiene como función principal apoyar el proceso de diseño, implementación y evolución de la arquitectura de TI en la F.G.N, para lograr que este alineada con las estrategias organizacionales y de más alto nivel. A continuación se muestra en un diagrama el contenido de este dominio:

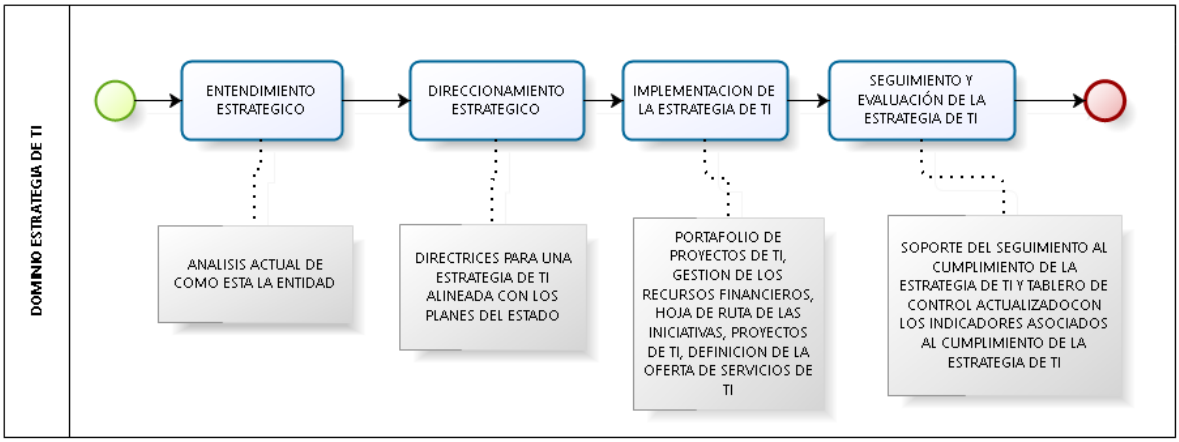


DIAGRAMA 1: DOMINIO ESTRATEGIA DE TI

FUENTE: INICIATIVA PROPIA

El mapa de ruta de proyectos de la Fiscalía incluye las necesidades de recursos, tiempo, alcance y costo para cada uno de ellos. La Fiscalía General de la Nación para esta vigencia y de acuerdo con las recomendaciones realizadas por la Dirección de Control interno como resultado de la auditoria ejecutada a finales de

octubre de la vigencia anterior, elaboró y se encuentra en proceso de aprobación el PETI (para la FGN PETIC), documento publicado en la web interna de la entidad en el mes de enero de 2017. Este documento contiene lo siguiente:

1- Objetivos
2- Alcance del documento
3- Marco Normativo
4- Análisis situación actual de la FGN, análisis que contiene los siguientes apartes:
    - Modelo Estándar de Control Interno (MECI)
    - Mapa de Procesos de la Entidad
    - Estrategias Sectoriales
    - Políticas FGN
    - Política de operaciones por procesos
    - Descripción actual de la Subdirección de Tecnologías de la Información y las Comunicaciones
    - Indicadores
    - **Riesgos (Describen los mismos que se encuentran publicados desde el año 2015 en el mapa de riesgos de la entidad),** es preciso indicar que el análisis y actualización de los mismos debe realizarse por lo menos una vez al año ya que estos son volátiles, inciertos, complejos y ambigüos [24].
    - Uso y apropiación de la tecnología
    - Sistemas de Información
    - Gobierno de TI
5- Modelo de planeación , donde establecen:
    - Arquitectura tecnológica
    - Consolidado de proyectos de Inversión

5.3.1.1 El Ámbito de entendimiento Estratégico

Es donde se busca el entendimiento preciso, claro y documentado de la situación actual de la F.G.N, en el contexto organizacional y su entorno, para que le permita a la Subdirección de las TICs usar la tecnología como agente transformador; los lineamientos son los siguientes:

- **Entendimiento Estratégico**: Estrategia de TI alineada con las estrategias sectoriales, plan nacional de desarrollo, la cual debe estar orientada a generar valor y contribuir al logro de los objetivos.

- **Definición de arquitectura empresarial**, para ello la entidad, debe aplicar el marco de referencia de Arquitectura para la gestión de TI definido en el país (*marco definido a partir de 6 dominios, no obstante las autoras de este proyecto proponemos la gestión de riesgos transversales a todos los procesos de la entidad para que el análisis de riesgos no solo se enfoque a los analizados en el área de TI, permitiendo la identificación de nuevos riesgos que puedan afectar e impactar a la entidad*).

- **Proceso para evaluar y mantener la arquitectura empresarial** la entidad debe Diseñar e implementar un proceso que permita evaluar y mantener actualizada la AE, de acuerdo con los cambios estratégicos organizacionales y tendencias de TI en la industria.

- **Mapa de ruta de la Arquitectura Empresarial,** Portafolio de proyectos priorizado y actualizado, incluye las necesidades de (tiempo, costo y alcance)

- **<u>Documentación de la estrategia de TI en el PETI</u>,** es decir se debe incluir dentro de este un capitulo anexo específico de tecnologías de la información.

<u>5.3.1.1.1 Evidencia o soporte de la implementación</u>:

- PETI (con proyección de la estrategia a 4 años y actualizado anualmente de acuerdo con los cambios de la estrategia en la entidad) donde se incorpore los objetivos de TI y los objetivos organizacionales de la FGN, documento que debe ser aprobado por el señor Fiscal General de la Nación.

- La arquitectura de TI en la FGN debe desarrollarse a partir de los 6 dominios del marco de referencia de AE para la gestión de TI.

- Portafolio de proyectos priorizado y actualizado de acuerdo con los resultados de arquitectura empresarial realizados en la entidad.

<u>5.3.1.1.2 Roles y Responsabilidades</u>

El responsable de la ejecución de las actividades de este ámbito es el CIO que en la Fiscalía sería el Subdirector de las TICs.

CIO – Subdirector de Tecnología de la Información y las Comunicaciones.

5.3.1.1.3 Diagrama ámbito de entendimiento estratégico en Bizagi

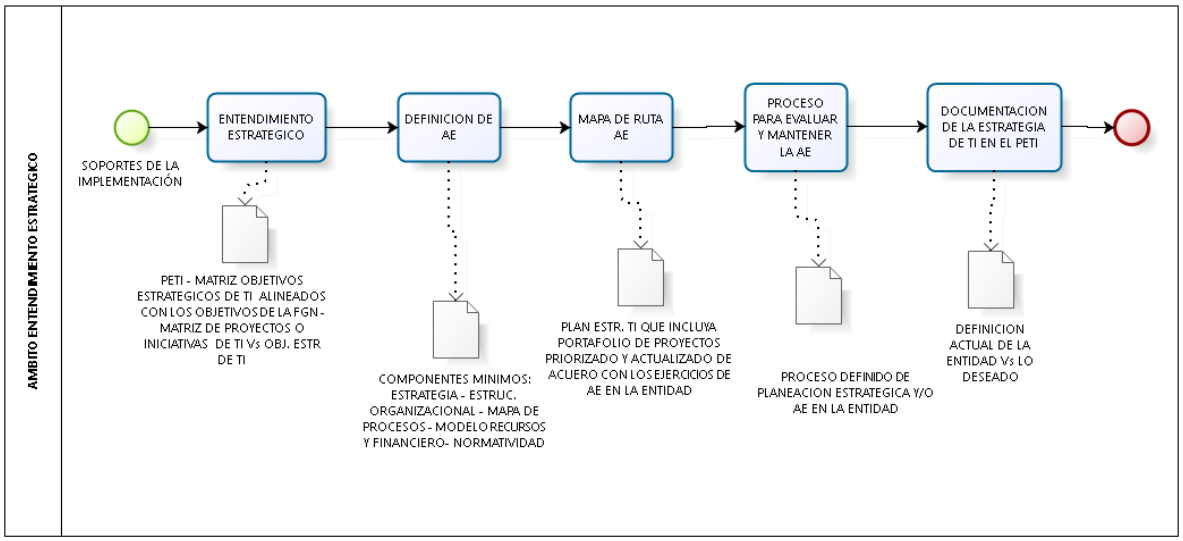


DIAGRAMA 2: AMBITO DE ENTENDIMIENTO ESTRATEGICO

FUENTE: INICIATIVA PROPIA

5.3.1.2 El Ámbito de Direccionamiento Estratégico

La FGN busca proporcionar pautas para una estrategia de TI alineada con los planes del Estado, los sectoriales e institucionales. Este ámbito contiene la identificación de retos y oportunidades de TI, así como la definición de política e iniciativas estratégicas de TI, los lineamientos son los siguientes:

- La subdirección de las TICs debe identificar y definir las políticas y estándares que faciliten la gestión y gobernabilidad de TI, documento que debe contener los siguientes temas: seguridad de la información, continuidad del negocio, gestión de la información, adquisición, desarrollo e implementación de sistemas de información, acceso a la tecnología por parte de los usuarios (servidores / funcionarios).

- La subdirección de las TICs debe definir un plan de comunicación de la estrategia y la gestión de TI

5.3.1.2.1 Evidencia o soporte de la implementación:

- Plan de comunicaciones (documento aprobado a través de acto administrativo). Los soportes presentados por Subdirección de las TICs. deben coincidir con las actividades establecidas en dicho plan. El plan debe contener de manera clara: Roles, actividades, grupo de interés, frecuencia, canales de comunicación y los productos a desarrollar o salidas finales.

5.3.1.2.2 Roles y Responsabilidades

El responsable de la ejecución de todas las actividades de este ámbito es el CIO que en la Fiscalía seria el Subdirector de las TICs.

CIO – Subdirector de Tecnología de la Información y las Comunicaciones.

5.3.1.2.3 Diagrama ámbito de direccionamiento estratégico en Bizagi

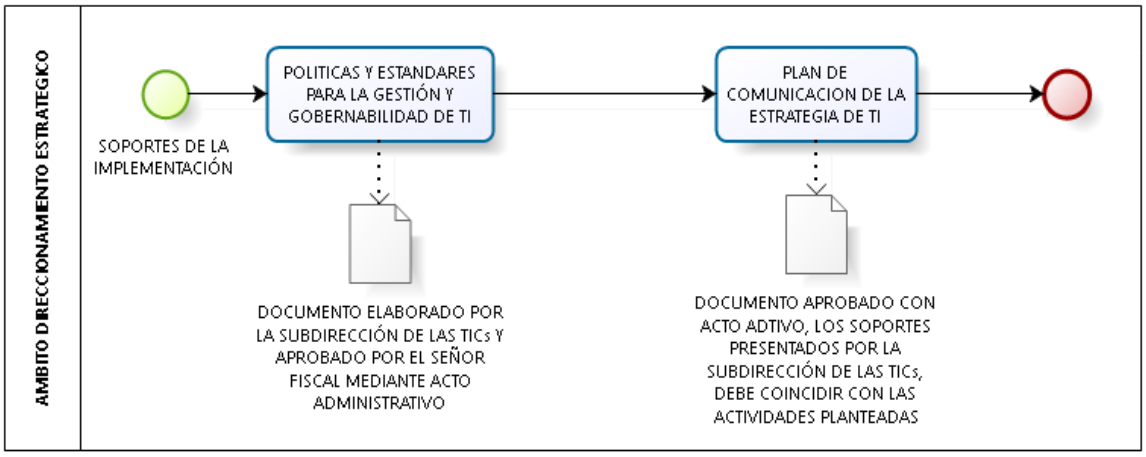


DIAGRAMA 3: DIRECCIONAMIENTO ESTRATEGICO

FUENTE: INICIATIVA PROPIA

5.3.1.3 El Ámbito Implementación Estrategia de TI

La entidad, con esto se busca el despliegue de proyectos estratégicos de TI y su entrega para la operación en la entidad. En este ámbito se incluye portafolio de proyectos de TI, gestión de recursos financieros, hoja de ruta de las iniciativas, proyectos de TI y contratos firmados de TI. Los lineamientos son los siguientes:

- Participación en proyectos con componentes de TI: se debe crear el comité de Arquitectura Empresarial en la FGN, a través de resolución expedida por el señor Fiscal General de la Nación. La Subdirección de las TICs como integrante con voz y voto debe participar activamente en la planeación y desarrollo de los proyectos de la entidad que incorporen componentes de TI.

- Control de los recursos financieros: La Subdirección de las TICs debe realizar seguimientos periódicos y control de la ejecución presupuestal de acuerdo con los proyectos asociados en el PETI (PETIC para la FGN 2017-2020).

- Gestión de proyectos de inversión: La Subdirección de las TICs debe formular, administrar, ejecutar y hacer seguimiento de las fichas de los proyectos de inversión.

- Catálogo de servicios de TI: La Subdirección de las TICs debe diseñar y mantener actualizado el catálogo de servicios de TI de acuerdo con el contrato de acuerdos de Nivel de Servicios (ANS) existente en la entidad.

5.3.1.3.1 Evidencia o soporte de la implementación:

- Análisis de impacto de los proyectos
- Acta de reunión comité de AE de la entidad
- Iniciativas de proyectos con el recibido

- Acta de seguimiento y cronogramas de los proyectos de TI
- Contratos de TI firmados
- Informes de supervisión compartida entre TI y otras áreas funcionales en los proyectos que tienen componentes tecnológicos que implican liderazgo de TI.
- Reportes, informes o acta de seguimiento y control de la ejecución presupuestal de los proyectos de TI asociados en el PETI de la entidad.
- Fichas de proyectos de inversión.
- Catalogo o portafolio de servicios de TI de la F.G.N. disponibles para la consulta.

5.3.1.3 .2 Roles y Responsabilidades

El responsable de la ejecución de todas las actividades de este ámbito es el CIO, junto con el responsable de la gestión de proyectos y el responsable de la gestión de la información que en la Fiscalía serían el Subdirector de las TICs, Jefe de Seguridad y Privacidad de la Información y el Gestor de proyectos de inversión.

CIO – Subdirector de Tecnología de la Información y las Comunicaciones.

Responsable Gestión de Proyectos – Gestor de proyectos de inversión

Responsable Gestión de la Información – Jefe de seguridad y privacidad de la información.

5.3.1.3.3 Diagrama ámbito implementación de la estrategia de TI en Bizagi

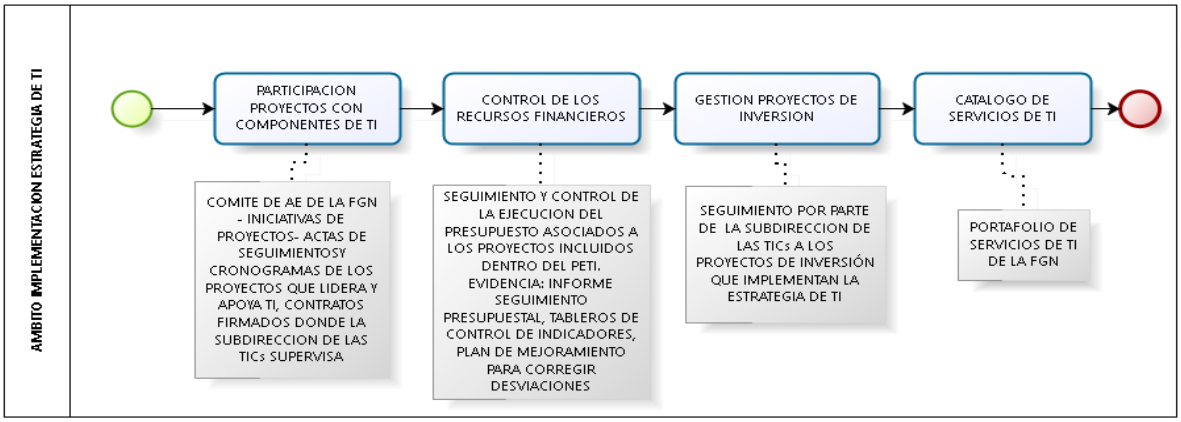


DIAGRAMA 4: IMPLEMENTACION DE LA ESTRATEGIA DE TI

FUENTE: INICIATIVA PROPIA

5.3.1.4 El Ámbito Seguimiento y Evaluación de la Estrategia de TI

La entidad, busca facilitar y asegurar un correcto seguimiento de la implementación de la estrategia de TI y cumplimiento de la entrega de valor a la entidad. Los lineamientos son los siguientes:

- La subdirección de las TICs debe realizar periódicamente la evaluación de la gestión de la estrategia de TI, con el fin de determinar el nivel de avance y cumplimiento de las metas definidas en el PETI.

- La subdirección de las TICs debe contar con un tablero de indicadores sectorial e institucional que permita tener una visión integral de los avances y resultados en el desarrollo de la estrategia de TI.

5.3.1.4.1 Evidencia o soporte de la implementación:

- Soportes del análisis y seguimiento a los indicadores asociados al cumplimiento de la estrategia de TI. La periodicidad de la medición y evaluación de los indicadores se recomienda en un tiempo no mayor a tres (3) meses. La asignación de fecha y responsables del seguimiento deben ser claras y precisas.

- Tablero de control actualizado.

5.3.1.4.2 Roles y Responsabilidades

El responsable de la ejecución de todas las actividades de este ámbito es el CIO, junto con el responsable de la gestión de la información que en la Fiscalía serian el Subdirector de las TICs, y el Jefe de Seguridad y Privacidad de la Información.

CIO – Subdirector de Tecnología de la Información y las Comunicaciones.

Responsable Gestión de la Información – Jefe de seguridad y privacidad de la información.

5.3.1.4.3 Diagrama ámbito seguimiento y evaluación de la estrategia de TI en Bizagi

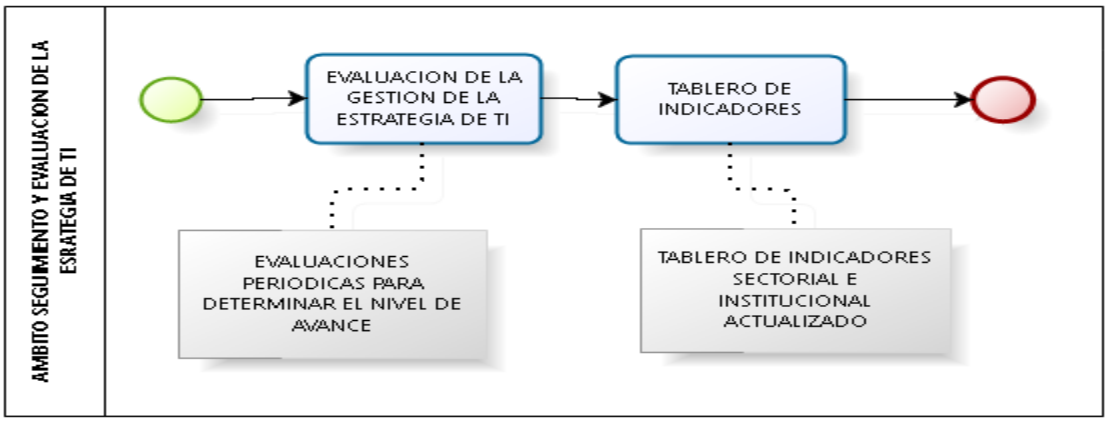


DIAGRAMA 5: SEGUIMIENTO Y EVALUACIÓN DE LA ESTRATEGIA DE TI

FUENTE: INICIATIVA PROPIA

5.3.2 DOMINIO GOBIERNO DE TI – APLICADO A LA ENTIDAD DE CONTROL (F.G.N)

A través de este dominio la entidad debe impartir directrices que permitan implementar esquemas de gobernabilidad de TI y para adoptar las políticas de seguridad de la información que se establezcan a partir de un acto administrativo (resolución) que el Señor Fiscal General de la Nación apruebe. Así mismo, permitirá alinear los procesos y planes de la entidad con los del sector.

5.3.2.1 Ámbito Cumplimiento y Alineación

Se busca con este ámbito asegurar el cumplimiento de la regulación y las políticas de TI por parte de los servidores y/o funcionarios de la entidad. Debe alinearse el modelo integrado por proceso existente en la FGN con los Riesgos, la regulación externa y el desarrollo e incorporación de las políticas de TI. Los lineamientos son los siguientes:

- Alineación del gobierno de TI: La subdirección de las TICs debe definir e implementar un esquema de Gobierno TI alineado con la estrategia misional y con el Modelo Integrado de Planeación y Gestión, que estructure y direccione el flujo de las decisiones de TI (Política de seguridad y privacidad de la FGN, actualmente tiene una política que fue aprobada con la resolución 0-4004 del 06 de noviembre de 2013, no obstante no se han presentado cambios y ajustes a la misma durante los últimos años por lo que debe ser objeto de análisis y actualización de acuerdo con lo establecido en las **condiciones de obligatoriedad del decreto 1078 de 2015, art. 2.2.9.1.1.1, en concordancia con el art. 1 del decreto 2573 del 2014 y el art. 39 de la ley 489 del 29 de diciembre de 1998** para la aplicación del marco de referencia en las entidades del Estado).

- Apoyo de TI a los procesos de la entidad: La subdirección de las TICs, debe apoyar la especificación de las necesidades de sistematización y demás apoyo tecnológico requerido por los diferentes procesos establecidos en la entidad, de tal manera que se incorporen facilidades tecnológicas que contribuyan a mejorar la articulación, calidad, eficiencia, seguridad, y a reducir los riesgos y los costos de operación.

- Conformidad: La subdirección de las TICs, debe definir e incorporar dentro de su plan estratégico, acciones que permitan corregir, mejorar y controlar procesos de TI que se encuentren dentro de la lista de no conformidades generada en el marco de las auditorias de control interno y externo, a fin de contribuir con el compromiso de mejoramiento continuo de la administración pública de la institución.

5.3.2.1.1 Evidencia o soporte de la implementación

- La FGN debe poseer una **política de TI actualizada, aprobada y comunicada**, acorde con la estrategia de la entidad y el sistema de gestión integral (S.G.I). La fecha de revisión o actualización registrada en el control de cambios no deberá superar un año (1) desde la última revisión. Así mismo dicha política debe ser comunicada a toda la entidad, esto se logra a través de correos masivos, jornadas de capacitación y/o presentación de la política de TI, concursos, protectores de pantalla, carteleras informativas, entre otras estrategias de comunicación.

- El esquema de la política de TI debe contener lo siguiente: objetivos, alcance, descripción de la política, responsables, definiciones, excepciones, seguimiento a las excepciones, evaluación de las excepciones, acto administrativo de aprobación de las excepciones, documentación de las excepciones, sanciones, referencias a otras políticas y normas que regulan o soportan la política.

- Modelo de gobierno de TI implementado; como soporte deben existir los siguientes documentos: el modelo de gobierno de TI, es un documento

maestro que puede hacer referencia a otros documentos y que debería contener, como mínimo, los procesos de gobierno de TI documentados, definición de roles y responsabilidades de TI, metodología de Gestión de Riesgos de TI, la estructura organizacional del área de TI y la estructura de decisiones de TI. El Esquema de gobierno alineado con el modelo conceptual definido en el dominio de Gobierno de TI del Marco de Referencia de AE, que se ilustra en la guía de generalidades. Entre los soportes documentales de implementación del esquema de gobierno se deben observar:

1. Actas de comité o instancia de gobierno de TI.
2. **Matrices y actas de seguimiento a los riesgos**.
3. Tableros de control para el seguimiento a proyectos de TI y la operación de TI.

- La subdirección de las TICs debe realizar un documento en el cual se pueda identificar, definir y especificar las necesidades de sistematización y apoyo tecnológico para cada uno de los procesos de la entidad a partir del mapa de procesos institucional, de tal manera que desde su diseño se incorporen facilidades tecnológicas que contribuyan a lograr transversalidad, coordinación, articulación, mayor eficiencia y oportunidad a nivel institucional y sectorial para obtener menores costos, mejores servicios, menores riesgos y mayor seguridad. (Documento de necesidades de sistematización y apoyo tecnológico a los procesos de la FGN - PETI).

- Definir indicadores sobre el impacto de las soluciones de TI, definir un plan de acción producto de la evaluación de las mediciones de los indicadores o impacto de las soluciones de TI.

- Definir plan de mejoramiento específico para las no conformidades decretadas por la Dirección de control interno y externo.

- Evidencias de seguimientos y soportes de las acciones correctivas definidas en el plan de mejoramiento para la atención de las no conformidades asociadas a la gestión de TI.

5.3.2.1.2 Roles y Responsabilidades

El responsable de la ejecución de todas las actividades de este ámbito es el CIO, que en la Fiscalía serian el Subdirector de las TICs.

CIO – Subdirector de Tecnología de la Información y las Comunicaciones.

5.3.2.2 Ámbito Marco o Esquema de Gobierno de TI

Permite al subdirector de las TICs, agrupar los elementos necesarios para establecer capacidades, procesos y esquemas de gobernabilidad de TI, bajo los cuales pueda monitorear, evaluar y redirigir las Tecnologías de la información de la entidad. **Los lineamientos** son los siguientes:

- Cadena de valor de TI: La subdirección de las TICs debe implementar dentro del mapa de procesos de la F.G.N un proceso llamado gestión de TI (La entidad actualmente tiene establecido este proceso y en la Figura 23: Estado

Actual Vs Deseado FGN de este documento, se describe) por otra parte el proceso de gestión de TI debe documentarse, actualizarse y ser publicado. La actualización del documento del proceso de gestión de TI no debe superar un año respecto de la última revisión.

- Capacidades y recursos de TI: La subdirección de las TICs debe definir, direccionar, evaluar y monitorear las capacidades disponibles y las requeridas de TI, las cuales incluyen los recursos y el talento humano necesarios para poder ofrecer los servicios de TI. (La capacidad de TI en la FGN se realiza de acuerdo con las necesidades en cada vigencia, así mismo se debe realizar una estimación para dos años y realizar la evaluación de la capacidad mensual- trimestral o anual en concordancia con el plan de acción). Es preciso aclarar que durante la vigencia 2016 hasta la fecha no se ha observado aumento en la capacidad de TI.

- Optimización de las compras de TI: La subdirección de las TICs debe realizar las compras a través de AMP[8] - Acuerdos Marco de Precios existentes [25] (en caso de que apliquen) y dar prioridad a adquisiciones en modalidad de servicio y/o por demanda. Debe además propender por minimizar la compra de bienes de hardware. (Invertir en la Gestión del conocimiento y la seguridad de los activos de información).

- Criterios de Adopción y de compra de TI: La subdirección de las TICs debe definir los criterios y métodos que direccionen la toma de decisiones de inversión en TI, buscando el beneficio económico y de servicio de la institución. Para todos los proyectos en los que se involucren Tecnologías de Información, se deberá realizar un análisis del costo total de propiedad de la

[8] Mediante los Acuerdos Marco de Precios (AMP), las entidades públicas han contratado servicios y productos por 229 mil millones de pesos, con excelentes condiciones de calidad, que además han permitido ahorros del 40% en promedio.

inversión, en el que se incorporen los costos de los bienes y servicios, los costos de operación, el mantenimiento, el licenciamiento, el soporte y otros costos para la puesta en funcionamiento de los bienes y servicios por adquirir. Este estudio debe realizarse para establecer los requerimientos de financiamiento del proyecto. Debe contemplar los costos de capital (CAPEX) y los costos de operación (OPEX). Para entender estos conceptos brevemente se expone el concepto realizado por el ***Dr. Luis Amendola, Ph.D, Dra. Tibaire Depool, PhD, María Castillo, GADE, MBA*** que dice:

"En toda organización uno de los objetivos principales es maximizar su rentabilidad; por lo tanto es muy importante tener en cuenta los costos que influyen tanto en el ciclo de vida de los activos que se poseen como en los proyectos que se realizan; para así poder tomar decisiones estratégicas. Por consiguiente se han de conocer y analizar las diferentes inversiones en las que se incurre a lo largo del ciclo: inversiones en adquisición o mejora de los bienes de capital (CAPEX) e inversiones asociadas al mantenimiento y otros gastos operativos (OPEX). La empresa debe de tener planificadas dichas inversiones para elaborar correctamente su presupuesto, por lo tanto es necesario tener en cuenta tanto la evolución de estas inversiones en ejercicios anteriores como las necesidades de todos los departamentos. Como consecuencia, las compañías se encuentran en ciertas ocasiones con la necesidad de sustituir CAPEX por OPEX y viceversa. Una vía de reducir dichos costos de capital por contrapartida de OPEX es el uso de la subcontratación o el alquiler de equipos e instalaciones. Las ventajas más evidentes de este cambio es el aumento de la flexibilidad de los costos y la reducción de las necesidades de financiación." [26].

- Retorno de la inversión de TI: La subdirección de las TICs debe establecer la relación costo beneficio y justificar la inversión de los proyectos de TI. Para establecer el retorno a la inversión, se deberá estructurar un caso de negocio para el proyecto, con el fin de asegurar que los recursos públicos se utilicen para contribuir al logro de beneficios e impactos concretos de la institución. Debido a la imposibilidad de obtener retorno monetario en la F.G.N, ya que se trata de gestiones sin ánimo de lucro, entre los beneficios deben contemplar resultados de mejoramiento del servicio, de la oportunidad, de la

satisfacción del ciudadano y del bienestar de la población, relacionado con la administración de justicia.

5.3.2.2.1 Evidencia o soporte de la implementación

- La Fiscalía General de la Nación, dentro del mapa de procesos tiene implementado el proceso de gestión Tecnológica y cuenta con la caracterización identificada con el siguiente código FGN-14.2-F-04, versión 1. Con última fecha de actualización 28/05/2015. Así mismo en dicha caracterización se tiene identificados los proveedores, las entradas o necesidades, principales actividades, responsables, tipo de actividad, salida producto y cliente.

- Como evidencias de las capacidades y recursos de TI la Fiscalía debe tener la elaboración de un plan de capacidad de TI para cada uno de los servicios de TI establecidos en el direccionamiento estratégico planteado por el señor Fiscal General de la Nación.

- La evidencia de la optimización de las compras de TI se establece cada vez que la entidad suscribe contratos de adquisición de servicios o bienes por AMP [25] o por contratos de adquisición de bienes o servicios en modalidad de servicio. (Contratos firmados y ejecutados en cada vigencia, en cumplimiento al plan de compras establecido)

- Como evidencia para el retorno de la inversión de TI en la fiscalía se tomaran los resultados de evaluaciones de alternativas de solución e inversión de TI, lo anterior basado a que en la entidad los beneficios se contemplan en el mejoramiento del servicio al ciudadano. (acceso a la justicia de forma oportuna).

5.3.2.2.2 Roles y Responsabilidades

El responsable de la ejecución de todas las actividades de los lineamientos cadena de valor de TI, Capacidades y recursos de TI, Criterios de Adopción y de compra de TI y retorno de inversión de TI es el CIO, que en la Fiscalía es el Subdirector de las TICs.

CIO – Subdirector de Tecnología de la Información y las Comunicaciones.

Los responsables de la ejecución de todas las actividades del lineamiento optimización de las compras de TI son:

CIO – Subdirector de Tecnología de la Información y las Comunicaciones en la Fiscalía.

Responsable de la gestión de información – Jefe de seguridad y privacidad de la información en la Fiscalía.

Responsable de los sistemas de información – Jefe dpto. Sistemas de información en la Fiscalía.

Responsable de los servicios tecnológicos – Jefe de atención Requerimientos informáticos en la Fiscalía.

Responsable de la seguridad de la información – Director de la seguridad de la información en la Fiscalía.

5.3.2.3 Ámbito Gestión Integral de Proyectos de TI

Busca la adecuada gestión de programas y proyectos asociados a TI. Incluye el direccionamiento de proyectos de TI, el seguimiento y evaluación de los mismos. Los lineamientos que componen este ámbito son los siguientes:

- Liderazgo de Proyectos de TI: La subdirección de las TICs debe liderar la planeación, ejecución y seguimiento de los proyectos de TI. En aquellos casos en que los proyectos estratégicos de la institución incluyan componentes de TI y sean liderados por otras áreas, la subdirección de las TICs deberá liderar el trabajo sobre el componente de TI conforme a los lineamientos de la Arquitectura Empresarial de la institución.

- Gestión de Proyectos de TI: El gestor de proyectos deberá evaluar, direccionar y monitorear lo relacionado con TI, incluyendo como mínimo los siguientes aspectos de los proyectos: alcance, costos, tiempo, equipo humano, compras, calidad, comunicación, interesados, riesgos e integración. Desde la estructuración de los proyectos de TI, y hasta el cierre de los mismos, se deben incorporar las acciones necesarias para gestionar los cambios que surjan.

- Indicadores de Gestión de los Proyectos de TI: El gestor de proyectos deberá monitorear y hacer seguimiento a la ejecución del proyecto, por medio de un conjunto de indicadores de alcance, tiempo, costo y calidad que permitan medir la eficiencia y efectividad del mismo.

5.3.2.3.1 Evidencia o soporte de la implementación

- La evidencia de la subdirección de las TICs para el liderazgo de los proyectos de TI son: cartas u oficios de proyectos enviados por las distintas áreas de la entidad, actas de seguimientos en los formatos establecidos en el BIT por el sistema de gestión integral, cronograma de los proyectos donde la subdirección de las TICs apoya o lidera. Cada proyecto de TI debe contar con la aprobación de la subdirección de las TICs mediante acto administrativo que lo soporte. Por otra parte los contratos firmados donde la supervisión está a cargo de la subdirección de las TICs o esta compartida con otras áreas funcionales de la entidad, en todo caso los proyectos de TI deben ser liderados por la subdirección de las TICs.

- Los soportes documentales como evidencia de la gestión de proyectos de TI se encuentran los siguientes: carpeta de los contratos de proyectos de TI, carpeta de los informes de supervisión de los contratos debidamente firmados por los supervisores o interventores.

- Para los indicadores de gestión de los proyectos de TI como evidencia se debe tener acta de reunión de seguimiento a los proyectos, pueden ser mensuales, trimestrales, semestrales y anuales.

5.3.2.3.2 Roles y Responsabilidades

El responsable de la ejecución de todas las actividades del lineamiento liderazgo de proyectos de TI y gestión de proyectos de TI es el CIO y el responsable de la gestión de proyectos que en la Fiscalía serian es el Subdirector de las TICs y el gestor de proyectos.

CIO – Subdirector de Tecnología de la Información y las Comunicaciones en la Fiscalía.

Responsable de la gestión de proyectos – Gestor de proyectos en la Fiscalía

Los responsables de la ejecución de todas las actividades del lineamiento indicadores de gestión de los proyectos de TI son:

CIO – Subdirector de Tecnología de la Información y las Comunicaciones en la Fiscalía.

Responsable de la gestión de la información – Jefe de seguridad y privacidad de la información en la Fiscalía

5.3.2.4 Ámbito Gestión de la Operación de TI

Busca la adecuada planeación, ejecución, monitoreo y mejora continua de la prestación de los servicios de TI que se prestan en la entidad, así como la mejora continua de los servicios de los proveedores. Los lineamientos que componen este ámbito son los siguientes:

- Evaluación del desempeño de la Gestión de TI: La Subdirección de las TICs debe realizar monitoreo y evaluación del desempeño de la gestión de TI, a partir de las mediciones de los indicadores del proceso de gestión tecnológica.

- Mejoramiento de los procesos: La Subdirección de las TICs debe identificar áreas con oportunidad de mejora de acuerdo con el direccionamiento

estratégico establecido en la Fiscalía con el fin de contribuir con el cumplimiento de los objetivos institucionales.

- Gestión de proveedores de TI: La Subdirección de las TICs debe administrar todos los proveedores y contratos cuyo objetivo sea el desarrollo de proyectos de TI. Para ello durante el proceso contractual se debe aplicar un diseño de dirección, supervisión, seguimiento y control y recibo a satisfacción de los bienes y servicios contratados.

- Transferencia de información y conocimiento: La Subdirección de las TICs debe gestionar la transferencia del conocimiento asociado con los bienes y servicios contratados por la Fiscalía. Para ello se debe contar con planes de formación y transferencia del conocimiento en caso de cambios en el recurso humano.

5.3.2.4.1 Evidencia o soporte de la implementación

Como evidencias para el cumplimiento de estos lineamientos la entidad debe tener lo siguiente:

- Indicadores de gestión de TI definidos y documentados (objetivo, formula, fuente donde se obtiene los valores del indicador, periodicidad, frecuencia y responsables), así mismo deben cumplir con los lineamientos establecidos en las guías para la definición de indicadores del DAFP (Departamento Administrativo de la Función Pública)

- Encuestas de satisfacción (formularios y/o formatos de encuestas de satisfacción) para el proceso de gestión tecnológica y/o instrumentos

utilizados para realizar mediciones que permitan evidenciar la evaluación del desempeño de la gestión de TI.

- Tableros de control con los resultados de mediciones de los indicadores de desempeño de la gestión de TI.

- Proyectos o iniciativas de mejoramiento de los procesos de TI que contribuyan al cumplimiento de los objetivos del direccionamiento estratégico.

- Para la gestión de proveedores de TI como evidencias se deben tener actas de aprobación, recibido a satisfacción de productos y servicios, documentos soportes de supervisión, seguimiento y control de los proyectos de TI, que evidencien gestión del proveedor. Todos estos soportes deben hacer parte de las carpetas de los contratos.

- La Fiscalía debe diseñar, aprobar e implementar un procedimiento obligatorio para la gestión y transferencia de conocimiento asociado a los bienes y servicios de TI contratados por la entidad. Así mismo, deben existir manuales publicados en el bit del Sistema de Gestión Integral, teniendo en cuenta las políticas de control de acceso a usuarios que estén definidas en las políticas de TI.

- Todos los proyectos de TI, cuando así lo requieran deben tener una documentación funcional y técnica de cada uno de los bienes y servicios contratados por la entidad publicados en un repositorio institucional.

- Actas de sesiones de transferencia, listas de asistencia a capacitación, y entrega de bienes y servicios de TI y recibido a satisfacción.

5.3.2.4.2 Roles y Responsabilidades

El responsable de la ejecución de todas las actividades de los lineamientos de este ámbito es el CIO o subdirector de las TICs para la Fiscalía, a excepción del lineamiento transferencia de información y conocimiento ya que el responsable de la gestión de la información que en la Fiscalía seria el jefe de seguridad y privacidad de la información.

CIO – Subdirector de Tecnología de la Información y las Comunicaciones en la Fiscalía.

Responsable de la gestión de la información – Jefe de seguridad y privacidad de la información en la Fiscalía.

5.3.3 DOMINIO DE INFORMACION – APLICADO A LA ENTIDAD DE CONTROL (FGN)

Este dominio en la entidad se puede decir que se encuentra establecido a través de la **resolución 0-1261 del 23 de julio de 2014**, ***"por medio de la cual se establecen***

directrices y se adoptan buenas prácticas, para el desarrollo, mantenimiento y calidad de los sistemas de información en la Fiscalía General de la Nación". Así mismo a través de la **resolución 0-4004 del 6 de noviembre de 2013**, ***"por la cual se actualizan las políticas de seguridad de la información, emitidas mediante la circular DFGN- 001 del 06 de mayo de 2006 por el señor Fiscal General de la Nación".*** No obstante no han sido actualizadas por lo que la subdirección de las TICs debe presentar a la instancia correspondiente la actualización de dichos documentos, para que sea revisada y aprobada con acto administrativo por el Señor Fiscal, más aún cuando la política de seguridad de la información en la entidad debe ajustarse con la normatividad vigente y los estándares internacionales sobre los cuales se fundamenta, los controles implementados para la mitigación de los riesgos, con el fin de garantizar que sea adecuada, suficiente y eficaz para la Entidad.

En este dominio se encuentran los siguientes ámbitos:

5.3.3.1 Ámbito Planeación y Gobierno de los Componentes de Información

Forma adecuada de planeación y gobierno de los componentes de información: datos, información, servicios de información y flujos de información. Los lineamientos para este ámbito son los siguientes:

- Responsabilidad y gestión de los componentes de información: la subdirección de las TICs debe definir directrices (fueron definidas a través de las resoluciones 0-1261 y 0-4004, no obstante no están actualizadas y solo se cumple en un 15% en la entidad lo anterior de acuerdo con resultados de auditoría realizada por la DCI en octubre y noviembre de 2016) y liderar la gestión de los componentes de información durante su ciclo de vida. Así mismo, trabajar en conjunto con las dependencias para establecer acuerdos que garanticen la calidad de la información. (Esto fue establecido a través de la resolución 0-126, no obstante en los resultados de la última auditoria

se evidenció, "*que existen sistemas de información, tales como, [9]SRAF, SIG y SISAC entre otros, que han sido desarrollados por la Dirección Nacional del Cuerpo Técnico de Investigaciones - CTI, que aún no están bajo la gobernabilidad de la Subdirección de Tecnologías de la Información y de las Comunicaciones; por lo tanto, se incumple con lo establecido en el artículo 8, de la resolución 0-1261 del 23 de julio de 2014, el cual dice: "La Subdirección de Tecnologías de la Información y de las Comunicaciones realizará todas las actividades tendientes a lograr el gobierno de los Sistemas de Información a fin de que los sistemas que han sido construidos por las dependencias de la Fiscalía General de la Nación, se incorporen y se integren a los sistemas misionales y/o de apoyo, ya institucionalizados")*

- Plan de calidad de los componentes de información: La subdirección de las TICs debe contar con un plan de calidad de los componentes de información que incluya etapas de aseguramiento, control e inspección, medición de indicadores de calidad, actividades preventivas, correctivas y de mejoramiento continuo de la calidad de los componentes.

- Gobierno de la Arquitectura de Información: La subdirección de las TICs debe definir, implementar y gobernar la Arquitectura de Información estableciendo métricas e indicadores de seguimiento, gestión y evolución de dicha arquitectura.

- Gestión de documentos electrónicos: La subdirección de las TICs debe contemplar el ciclo de vida de la gestión documental en la arquitectura de Información.

- Definición y caracterización de la información georreferenciada: La subdirección de las TICs debe acoger la normatividad, los estándares

[9] SRAF: Sistema para el Registro de Armas de Fuego en la entidad. SIG: Sistema de Información para la Gestión Técnico investigativa. SISAC: Sistema de información Sección Analisis Criminal.

relacionados de la Infraestructura Colombiana de Datos Especiales ([10]CDE) [27], los lineamientos de política de información geográfica y demás instrumentos vigentes que rijan la información geográfica según el comité técnico de normalización.

5.3.3.1.1 Evidencias o soportes de la implementación:

- Como se describió en el punto anterior en los lineamientos la fiscalía cuenta con un documento de política de TI, aprobado a través de la Resolución 0-4004 del 6 de noviembre de 2013, la cual debe ser objeto de actualización ya que la misma según lo establece MINTIC en el modelo de AE este documento debe ser actualizado y aprobado en un periodo que no deberá superar un año (1).

- La entidad debe tener un documento del modelo o esquema de gobierno de la información que contenga como mínimo, custodios y responsables, calidad de los datos, migración de datos y datos maestros. El modelo debe estar acompañado de un plan de implementación y evidencias acorde con el plan definido.

[10] La Infraestructura Colombiana de Datos Espaciales - ICDE se define como un órgano de articulación, que gestiona la producción y el acceso a la información geográfica, a través de acciones coordinadas entre el Gobierno y la Sociedad, que promueven la implementación de políticas, la estandarización y el desarrollo de estrategias orientadas a la accesibilidad e interoperabilidad de recursos geoespaciales*, como base para la toma de decisiones.

*Recursos geoespaciales. Son recursos heterogéneos (datos, información, software, metadatos, servicios, estándares, marco legal, acuerdos, políticas) de carácter geoespacial.

- Componentes
- Comunidad
- Datos
- Fortalecimiento institucional
- Estándares
- Políticas
- Tecnologías

- Con relación al gobierno de arquitectura de información debe contener lo siguiente:

  - ✓ Matriz RACI (esta matriz ya fue definida en este documento en la fase II).

  - ✓ Indicadores de gestión, esquema de toma de decisiones de la arquitectura de la información.

  - ✓ Gestión de Riesgos con relación a la arquitectura empresarial.

- Definición de roles y perfiles para los servidores que desempeñen funciones de gestión de los componentes de información.

- Definir un documento que soporte los acuerdos entre áreas o dependencias.

- Definir y diseñar un plan de calidad el cual se aprobado por la instancia correspondiente.

- La evidencia para el lineamiento de gobierno de la arquitectura de información es un documento del Modelo de Gobierno de Arquitectura de Información.

- Para la gestión de documentos electrónicos la entidad cuenta con un procedimiento interno para la gestión de documentos y expedientes electrónicos, los cuales pueden ser consultados en la intranet proceso de gestión documental.

5.3.3.1.2 Roles y Responsabilidades:

Los responsables de la ejecución de todas las actividades de los lineamientos de este ámbito y los demás que se describen para este dominio son:

CIO – Subdirector de Tecnología de la Información y las Comunicaciones en la Fiscalía.

Responsable Gestión de Proyectos – Gestor de proyectos en la Fiscalia.

Responsable análisis y generación de la información – Jefe dpto. Sistemas de información en la Fiscalía.

Analista del diseño de componentes de información – Jefe de Comunicaciones en la Fiscalía.

Responsable Aseguramiento de la Calidad – Asesor de procesos y aseguramiento de la calidad en la Fiscalía.

Responsable del cumplimiento – Director Arquitectura Empresarial en la Fiscalía.

5.3.3.2 Ámbito Diseño de los Componentes de Información

Busca la adecuada caracterización y estructuración de los componentes de Información. Los lineamientos para este ámbito son los siguientes:

- Lenguaje común de intercambio de componentes de información: La subdirección de las TICs debe, utilizar un lenguaje común para el intercambio de información con otras instituciones, para ello deberá solicitar la incorporación de nuevos elementos de datos en el lenguaje común de intercambio de datos cuando aplique.

- Directorio de servicios de componentes de información: La subdirección de las TICs debe, crear y mantener actualizado un directorio de los componentes de información.

- Publicación de los servicios de intercambio de componentes de información: La subdirección de las TICs debe, publicar los servicios de intercambio de información a través de la plataforma de interoperabilidad del estado colombiano.

- Canales de acceso a los componentes de información: La subdirección de las TICs debe, garantizar los mecanismos que permitan el acceso a los servicios de información por parte de los diferentes grupos de interés, contemplando características de accesibilidad, seguridad y usabilidad (Gobierno en línea).

5.3.3.2.1 Evidencias o soportes de la implementación

Como evidencias de implementación de cada una de las actividades de estos lineamientos se tiene:

- Certificado de nivel 2 o 3 de lenguaje común para el intercambio de datos. Se evidencia a través del portal de lenguaje de intercambio de datos entre las instituciones.

- Directorio de componentes de información actualizado.

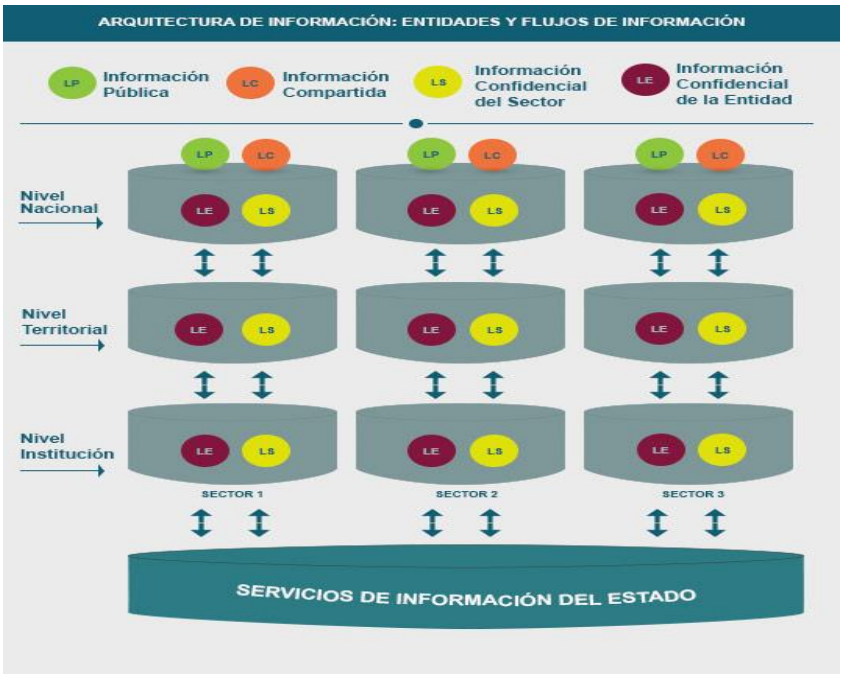
- Web services publicados en la plataforma de interoperabilidad del estado colombiano (inventario y directorio actualizado de los componentes de

información que tiene la entidad), lo anterior teniendo en cuenta que información por normatividad debe producir oficialmente y esta se convierta en un servicio de información publicado en la PDI[11] (Plataforma de Interoperabilidad (**PDI**) que permite compartir información entre entidades) [28], a continuación se muestra modelo diseñado por MINTIC para entenderlo:

[11] Colombia cuenta con la Plataforma de Interoperabilidad (PDI) que permite compartir información entre entidades. La evolución de la PDI busca estandarizar los flujos de dicha información, la capacidad para transformar los datos desde una fuente a un receptor y la gestión de los procesos inherentes al intercambio que garanticen la calidad, la trazabilidad y el uso.

Actualmente, el costo de intercambio de información es muy alto debido a la diferencia de representación de datos en diversos sectores. Si bien cada sector se encuentra en un distinto nivel de madurez en la gestión de información, los requisitos mínimos de calidad deben alcanzarse prontamente, de tal modo que se puedan exponer conjuntos de información útil para otras entidades.

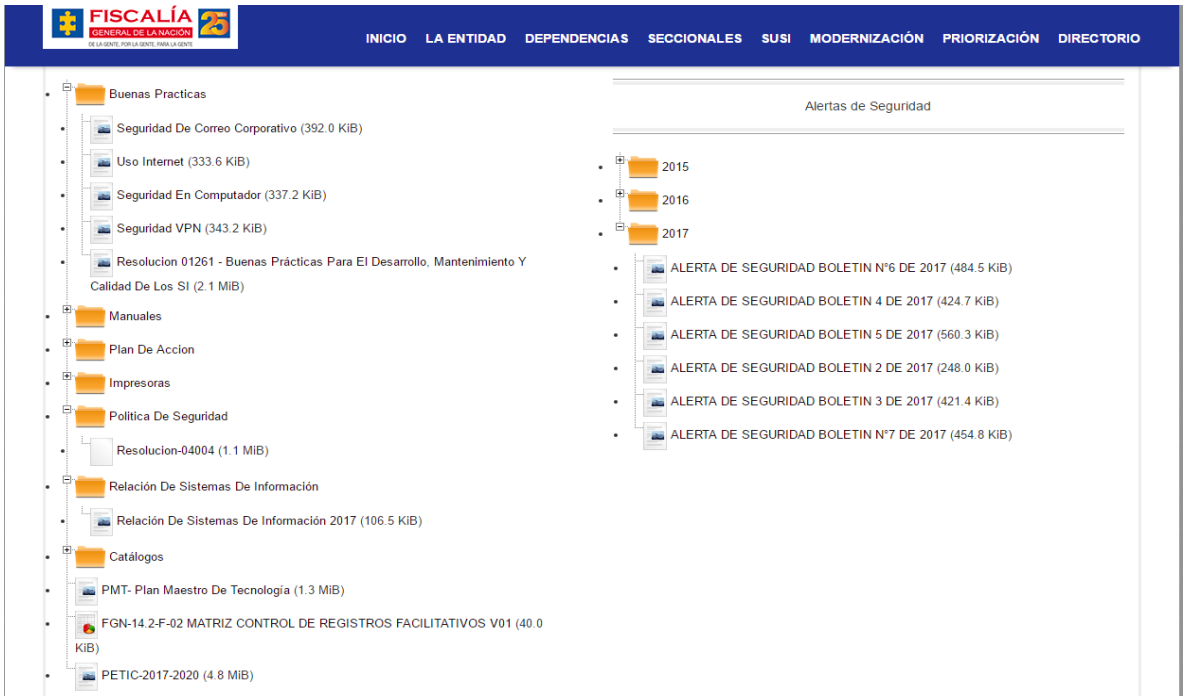
El intercambio supone un ejercicio real de reutilización con calidad de la información disponible, de manera que los datos puedan obtenerse a bajo costo y con la representación estándar para reducir el desarrollo de software y para usar la información desde fuentes externas. Una vez se tenga un esquema de interoperabilidad ampliamente generalizado y estandarizado, se puede pensar en tener un sistema integrado en el Estado.



Fuente: http://www.mintic.gov.co/gestionti/615/w3-propertyvalue-6274.html

- Catálogo de componentes de información el cual debe contener los siguientes atributos: Caracterización de los servicios, grupos de interés, canales de acceso, características de accesibilidad (los contemplados en la norma NTC 5854 según nivel definido por la FGN), seguridad (lo establecido en la FGN para la seguridad y los accesos – Norma ISO 27000) y usabilidad (lo contemplado en GEL).

- Actualmente la entidad cuenta con el siguiente repositorio de información, el cual se encuentra ubicado en la ruta: http://web.fiscalia.col/fiscalnet/fiscal-general-de-la-nacion/direccion-nacional-de-apoyo-la-gestion/subdireccion-tecnologias-de-la-informacion-y-de-las-comunicaciones/.



Fuente: repositorio de información de la FGN – Subdireccion de las TICs

Por otra parte, la Fiscalía General de la Nación tiene una página web para el servicio al ciudadano, cumpliendo con los parámetros establecidos en la norma NTC 5854 para la entidad y de acuerdo con lo establecido en la normatividad para el gobierno en línea.

Fuente: http://www.fiscalia.gov.co/colombia/

5.3.3.2.2 Roles y Responsabilidades:

Los mismos que se describen en el punto **5.3.3.1.2,** de este documento.

5.3.3.3 Ámbito Diseño de los Componentes de Información

Permite a la entidad orientar y estructurar procesos de análisis para la toma de decisiones a partir de los componentes de información que se procesa. Los lineamientos para este ámbito son los siguientes:

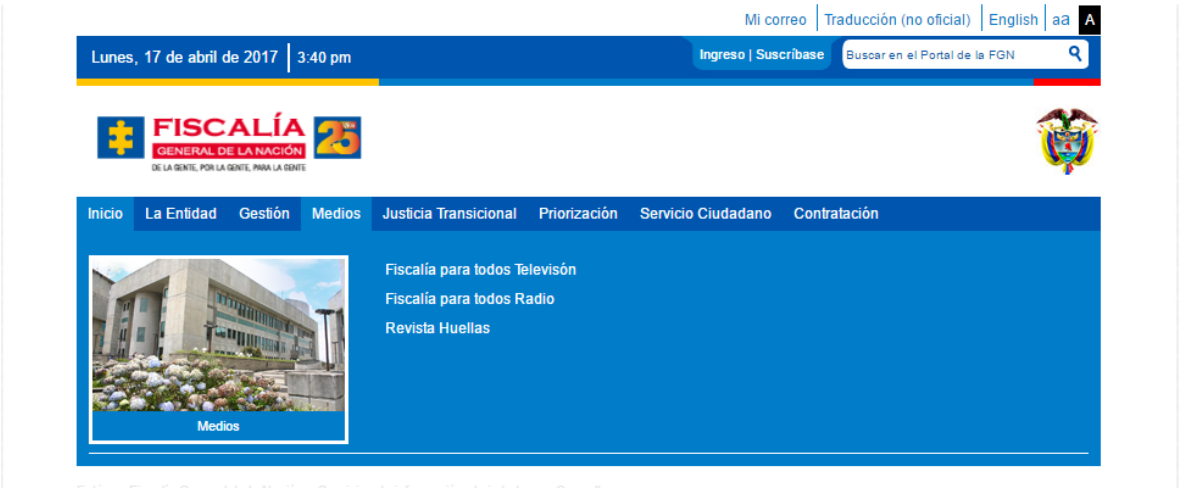
- Mecanismos para el uso de los componentes de información: La subdirección de las TICs debe implementar mecanismos que impulsen el uso de los servicios de información.

- Acuerdos de intercambio de información: documentos de los acuerdos de niveles de servicio (ANS) vigentes para el intercambio de información.

- Fuentes unificadas de información: catálogo de componentes de información donde este identificadas las fuentes oficiales y únicas de información. (inventario de componentes de información actualizado mínimo cada 6 meses)

5.3.3.3.1 Evidencias o soportes de la implementación

- La fiscalía a través de la página web proporciona mecanismos para recibir retroalimentación de los ciudadanos, en cuanto a calidad u oportunidad de la información.



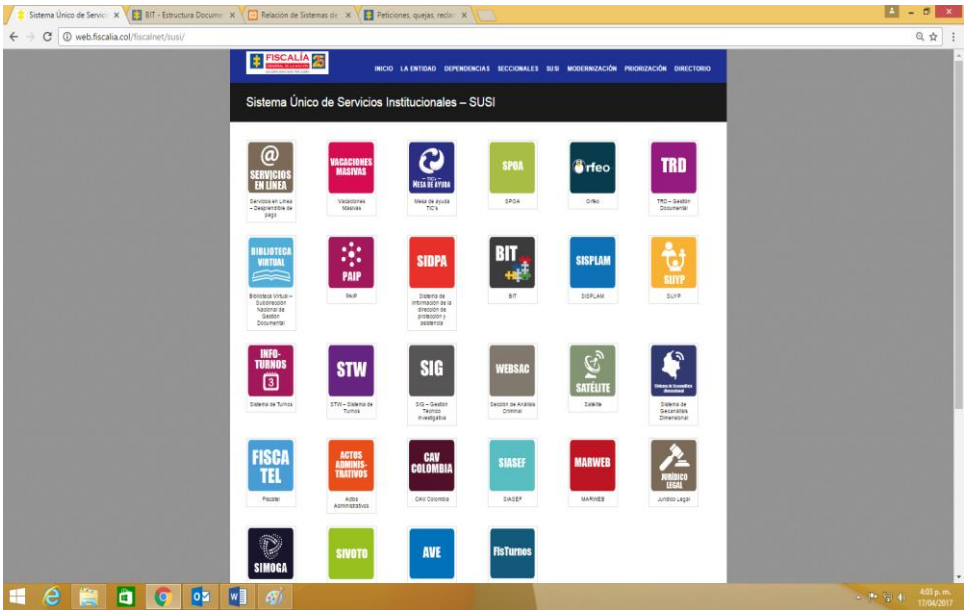
Fuente: http://www.fiscalia.gov.co/colombia/servicios-de-informacion-al-ciudadano/consultas/

Fuente: http://www.fiscalia.gov.co/colombia/servicios-de-informacion-al-ciudadano/consultas/

- L a entidad cuenta con un catálogo de servicios a través de la mesa de ayuda se pueden identificar los ANS de servicios establecidos a través del contrato CN- 0490 del 2014 con la empresa COMWARE– COMPUFACIL. (Información que fue buscada en la página del SECOP, y es información de carácter público)

FUENTE: http://10.44.65.68/USDK/Main/Pages/Categorys.aspx

- La entidad a través de la intranet tiene identificados el catálogo de componentes de información.



Fuente: http://web.fiscalia.col/fiscalnet/susi/

5.3.3.3.2 Roles y Responsabilidades:

Los mismos que se describen en el punto **5.3.3.1.2,** de este documento.

5.3.3.4 Ámbito Calidad y Seguridad de los Componentes de Información

Definición y gestión de los controles y mecanismos para alcanzar los niveles requeridos de seguridad, privacidad y trazabilidad de los componentes de información. Los lineamientos para este ámbito son los siguientes:

- Hallazgo en el acceso a los componentes de información: La subdirección de las TICs debe generar mecanismos que permitan a los usuarios de la información reportar los hallazgos encontrados durante el uso de los servicios de información.

- Protección y privacidad de los componentes de información: La subdirección de las TICs debe incorporar un catálogo de componentes de información teniendo en cuenta la normatividad que rige la protección y privacidad de la información.

- Auditoria y trazabilidad de componentes de información: La subdirección de las TICs debe definir criterios necesarios para asegurar la trazabilidad y auditoría sobre las acciones de creación, actualización, modificación o borrado de los componentes de información, los sistemas de información deben implementar estos criterios.

5.3.3.4.1 Evidencias o soportes de la implementación

La evidencia de implementación de los lineamientos de este ámbito son los siguientes:

- Debe existir un documento con el proceso de gestión de incidentes que contenga como mínimo: alcance, política de operaciones del proceso,

recursos del proceso, roles y responsabilidades, procedimientos e indicadores. En la entidad se cuenta con el proceso de Gestión Tecnológica más no de gestión de incidentes.

- Como mecanismos para el reporte de hallazgos sobre los servicios de información se puede tomar el modula de la mesa de ayuda – reporte de incidentes aplicaciones (software) ya sean por vía web o telefónicamente. (reporte a través de la mesa de ayuda de la entidad o informes de auditorías).

- La subdirección de las TICs, en el catálogo de componentes de información, debe incluir los responsables (custodio y dueño) de la protección y privacidad de la información de acuerdo con la normatividad de protección de datos personales y de acceso a la información pública. Se debe tener especial cuidado con la información en la entidad, lo anterior a que se manejan datos confidenciales y sensibles. (Ley 1581 DE 2012 - Por la cual se dictan disposiciones generales para la protección de datos personales y se reglamenta parcialmente por el decreto 1317 DE 2013). Así mismo el decreto 103 del 20 de enero de 2015, Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.

- Las evidencias para el cumplimiento de los lineamientos de auditoria y trazabilidad de los componentes de información, son los informes de auditoría de los sistemas de información, teniendo en cuenta que dichas auditorias se desarrollaran después de la implementación del marco de Arquitectura Empresarial.

5.3.3.3.2 Roles y Responsabilidades:

Los mismos que se describen en el punto **5.3.3.1.2,** de este documento.

5.3.4 DOMINIO SISTEMAS DE INFORMACION – APLICADO A LA ENTIDAD DE CONTROL (FGN)

En el dominio de sistemas e información se planea y diseña la arquitectura, el ciclo de vida, las aplicaciones, los soportes y la gestión de los sistemas, con el fin de que presten un servicio adecuado a la entidad y sean de apoyo para el logro del direccionamiento estratégico.

Se definen algunos principios ya definidos en los diferentes estándares para los sistemas de información así mismo se complementan con los aportes personales y los ya establecidos en la entidad, que deberán seguir los datos tanto en la arquitectura actual como en la futura y deben ser tenidos en cuenta siempre que se planee cualquier expansión sobre la arquitectura.

Definición de requerimientos

- Dimensionamiento de recursos de hardware y software (Arquitectura)
- Análisis y diseño del software
- Desarrollo
- Implementación y prueba de unidades
- Integración del sistema
- Operación y mantenimiento (Release)
- Actualización de fuentes
- Control de versiones
- Los datos que se almacenen deben ser adecuados y pertinentes.

- Los datos que se almacenen no deben ser excesivos.
- Los datos siempre deben tener una finalidad específica.
- El tiempo de almacenamiento de los datos debe ser estimado de acuerdo a la criticidad de la información que se maneja para el manejo de la Noticias criminales.
- En caso de realizar tratamiento de datos personales, esta debe cumplir los lineamientos existentes para la legislación Colombiana (normatividad descrita en el dominio anterior)
- Todos los datos almacenados deben tener niveles de privilegio para ser accedidos orientados a roles o perfiles dentro de los sistemas de información.
- Se debe evitar la duplicidad de información en diferentes sistemas.
- **La información debe estar debidamente respaldada y se debe contar con un plan de contingencia, lo anterior basado en la gestión de Riesgos. (La FGN como plan de mejoramiento de auditoria interna y externa tiene en ejecución el contrato**
- Se deben cumplir los principios de seguridad de la información que garanticen sus características de integridad, confidencialidad y disponibilidad (Norma ISO 27000).
- Monitoreo del sistema
- Recuperación del sistema
- Validación de fallas de funcionamiento de datos (software)
- Corrección de fallas de funcionamiento de hardware
- Desarrollo de mejoras del sistema
- Corrección de errores de usuario
- Corrección de errores del sistema

- Atención a usuarios
- Actualización de software (Release y Patches)
- Creación, borrado, activación o modificación de perfiles y usuarios
- Asesorar en el desarrollo de sistemas nuevos o mejorados
- Soporte al sistema operativo
- Recopilación y análisis de estadísticas de la información
- Bodega de datos e inteligencia de negocios
- Recopilación y análisis de estadísticas del sistema
- Extracción y cargue de datos

A continuación se describen los diferentes sistemas de información que actualmente gestiona los procesos estratégicos, misionales, de apoyo y de seguimiento control y mejora en la Fiscalía:

Listado de Sistemas de Información FGN	
Nombre	**Descripción**
SPOA Sistema de Información Sistema Penal Oral Acusatorio	Descripción general Apoyo a la gestión del área de Fiscalía Actuación Procesal Ley 906/2004. Permite el registro de las noticias criminales. Controla la carga laboral de los SPOA Sistema de Información Sistema Penal Oral Acusatorio fiscales mediante la asignación de los casos, facilita la gestión de las noticias para los fiscales y la policía judicial. Controla el manejo de las evidencias.

SIJUF Sistema de Información judicial de la Fiscalía	Actuación Procesal / Ley 600 de 2.000 Apoyar a los directores de Fiscalías y Jefes de Unidad en el cumplimiento de su función de control de gestión en cada una de sus unidades. Herramienta tecnológica de soporte al proceso de distribución de carga laboral a Fiscales delegados que permite: *Distribuir equitativamente las Investigaciones *Generar reportes para el Control de Gestión
SIRED	Permitir el registro de la información de Quejas, Despachos Comisorios y Procesos Disciplinarios que lleva la Oficina de Veeduría. Permite hacer el reparto de las diligencias en forma aleatoria de acuerdo a la carga laboral de los abogados, permite distribuir equitativamente las Investigaciones, generar reportes para el Control de Gestión. Herramienta tecnológica de apoyo a la Oficina de Veeduría y a los Grupos de Control Interno Disciplinario
SICVI Sistema de información de control de visitantes	Permitir el control de ingreso de los visitantes los cuales son validados con la base de datos del sistema SIAN. Adicionalmente permite el ingreso de funcionarios que no portan el carnet, bajo la categoría de visitante especial. Es un sistema de apoyo a sedes del Área Administrativa, Fiscalías y CTI.
SIAN Sistema de Información de Antecedentes y Anotaciones	Es un sistema de Información Judicial que apoya la labor misional en los despachos de fiscalías, Jueces y funcionarios con funciones permanentes o transitorias de Policía Judicial. Registro de antecedentes y

	anotaciones judiciales en contra de las personas.
EVIDENTIX	Tiene como objetivo integrar la información de las diferentes labores propias de la investigación.
	Es un sistema de información de apoyo a la labor del CTI.
SIAF Sistema de Información Integrado Administrativo y Financiero	Es la herramienta que apoya la gestión del área administrativa y financiera de la FGN. Es un SI, adaptado por la Oficina Informática a la medida, cubriendo las necesidades de las dependencias administrativas y financieras de la FGN, de forma integrada. Es una herramienta descentralizada con bases de datos distribuidas en las 25 seccionales administrativas y financieras del orden nacional y cuenta con los procedimientos para consolidar dicha información.
STARSISO	Es un sistema de información gerencial importante para la toma de decisiones relacionadas con el talento humano, los procesos de trabajo y el clima organizacional. Suministra información básica para la determinación del perfil epidemiológico de la entidad, y definición de los índices de ausentismo y accidentalidad. Se encuentra instalado en todo el país y se constituye en base de liquidación mensual de nómina. Permite realizar procesos de consolidación.

ORFEO Sistema de Gestión Documental.	Permite el registro, digitalización, clasificación, organización, agrupación, trámite, almacenamiento, recuperación y trazabilidad de los documentos al interior de las dependencias
BIT: Business Información Technology:	Sistema que apoya el Sistema Integrado de Gestión de la Calidad. En este este portal ubicado en la INTRANET y permite la consulta de todos los documentos relacionados con el proceso de Gestión de Calidad de la entidad y del MECI
SISTEMA GEOREFERENCIAL	Integrar la información de las bases de datos de toda la entidad, llevarla a una bodega de datos espacial y manejarla en forma georreferenciada o espacial en páginas web para generar informes estadísticos, espaciales, multitemáticos, multitemporales, gráficos y realizar análisis OLAP en tiempo real permitiendo a los diferentes niveles de la Fiscalía General de la Nación la toma de decisiones.
SIJYP Transitorio (Actual)	Sistema de Información de justicia y Paz
Portal Web Fiscalía General de la Nación	Página Web de la Fiscalía General de la Nación a partir de la página actual, incluyendo el desarrollo, la puesta en funcionamiento de servicios de interés a la comunidad en general y la migración de la información actual a la nueva plataforma.
SIASEF	Sistema de información para la administración del programa de seguros
SIPRAIN	Sistema de Información de intercambio de pruebas de asuntos Internacionales

FISCALNET	Portal web interno que ofrece servicios a los funcionarios de la misma
JURIDICO LEGAL	Sistema de apoyo a la Oficina Jurídica
SISPLAM	Sistema de información para el registro del plan de mejoramiento suscrito con la CGR .
SIIF NACION	Sistema de Información Financiera diseñado y administrado por el Ministerio de
	Hacienda y Crédito Público
SISAC	Sistema para relacionar casos y atención de análisis criminal. Correlaciones bienes, personas para análisis
SIVOTO	Sistema de Información para elecciones por medio de votación electrónica.
SIDPA	Aplicación que permite el manejo de la información de casos de protegidos por la DNPyA del nivel nacional, así como el manejo de estadísticas e indicadores.
CRIF	Sistema que permite generar un repositorio de información de acuerdo con una matriz de variables definidas para el análisis, información que se extrae de diferentes dispositivos relacionada con grupos armados, fuentes de financiamiento, bienes, personas relacionadas a dichos bienes que pertenecen o tienen un rol en los grupos armados.
Actos Administrativos	Repositorio de documentos escaneados de actos administrativos de interés general

SISTEMA SIGTURNOS implementado a nivel nacional (en construcción reportes, consultas y tablero de control de monitoreo)	Sistema de Atención al Público en las Salas de Recepción de Denuncias SRD y Salas de Atención a Víctimas de la DNJT. Permite el manejo de sala de atención de usuario y brinda funcionalidades de asignación de turnos, calificación del servicio, registro de orientación y reportes estadísticos.
SCB	Sistema de comparación Balística es un sistema que funciona a nivel nacional para el cruce los casos de homicidio en donde se ven inmersas armas de fuego por medio de visión artificial, tiene módulos encargados de análisis, almacenamiento y correlación de los EMP vainillas, como fue un desarrollo interno en el CTI se realizó el registro de inscripción en la Dirección Nacional de derechos de autor es 1-2012-42095. Para el desarrollo de este software se realizó una convocatoria inicial a los principales proveedores de óptica en el país y finalmente fue la marca LEICA quien se ajustó a las necesidades estandarizadas para la captura y posicionamiento de los elementos balísticos ingresados y digitalizados en la base de datos.
Evaluación del desempeño	Permite parametrización, registro de evaluados y evaluadores, concertación de metas y calificaciones.
PQR'S	Modulo que permite el registro de peticiones, quejas y reclamos.
SRAF	SRAF sistema de registro de armas de fuego del Cuerpo técnico de investigación, todas las armas asignadas, los permisos de porte, y

	las diferentes novedades, como la asignación, perdida, prestamos, etc., se diseñó, desarrollo e implemento desde el mes de diciembre de 2012 el sistema de registro de Armas de Fuego SRAF, el cual se creó como un módulo dentro la página de la SAC Nivel Central, lo anterior aprovechando la infraestructura existente en cuanto a software, servidores, red y seguridad. Para el ingreso se debe digita en Internet Explorer la IP 10.1.7.240 o WebSac
SIMOGA	Herramienta que permite mediante elementos como código de barras realizar los inventarios de elementos asignados a los funcionarios, esta funcionalidad incluye traslados entre funcionarios.
MESA DE AYUDA - ARANDA	Herramienta de colaboración que permite implementar nueve procesos de ITIL en la Fiscalía General de la Nación, para llevar el registro de solicitud y atención de servicios, actualmente están configurados los servicios de TI, posteriormente se implementaran servicios de transportes y de administración de la sede.
CAV COLOMBIA	Herramienta que permite llevar el registro de información de víctimas, llevar el registro de las visitas, consultas y notificaciones
FEAB	Sistema de Información que permitirá la administración de los bienes que sean declarados mostrencos o vacantes y adjudicados a la Fiscalía General de la Nación o al Fondo por parte de autoridad competente, en los

	términos del artículo 89 de la Ley 906 de 2004. Los bienes sobre los cuales se haya reconocido la prescripción especial adquisitiva de dominio a favor de la Fiscalía General de la Nación o del Fondo por parte de autoridad competente, en los términos del artículo 89 A de la Ley 906 de 2004. El producto de la enajenación, frutos, dividendos, utilidades, intereses, rendimientos, productos y demás beneficios que se' generen de los bienes antes relacionados o de su administración. Los bienes que sean declarados administrativamente abandonados por el Fondo Especial para la administración de bienes de la Fiscalía General de la Nación previo agotamiento del procedimiento para su devolución previsto en la ley.
SIG-CTI y Especializadas.	Sistema que permite el registro misional de órdenes de trabajo, indicadores, secuencia, desplazamientos.
SIG- SECCIONALES	Sistema que permite el registro misional de órdenes de trabajo, indicadores, secuencia, desplazamientos. Sig, seccionales, casos de orden público en elecciones. Organizaciones Criminales
@nalisys	Los módulos con los que cuenta son los siguientes:
	Búsqueda de Noticia Criminal y complementa la información adicional que no se registra en SPOA y otra que viene de SPOA, necesaria para generar los formatos de: Formulario de

	Vehículos Hurtados (Características Detalladas).
	Formulario de Identificación de la Noticia Criminal y hechos. Formulario e
	Elementos Hurtados (Características Detalladas). Formulario de Testigos
	(Características Básicas y Descriptivas). Formulario de Víctimas (Características Básicas y Descriptivas). Formulario de Denunciantes (Características Básicas y Descriptivas). Formulario de ciado (Características Básicas y Descriptivas).
	Formulario de Imputados (Características Básicas y Descriptivas). Formulario de
	Delitos Informáticos (características específicas). Reportes
	- Constancias de Hurto de Automotores: Son documentos generados en formato PDF los cuales se remiten en algunos para la Ciudadanía o Entidades Competentes.
	- Generación de documentos combinados a través de una macro, la cual tomo como insumo el reporte en plano generado según los filtros del usuario, y mediante plantillas que cumplen con los formatos del SGI, combinan los registros y producen documentos masivos listos para ser firmados, esto es valor agregado para la unidad que dentro de su

	gestión debe realizar esta documentación según las continuas solicitudes de las entidades competentes. Aproximadamente se producen 2000 documentos mensuales aproximadamente, estadística que viene aumentando debido al crecimiento de los usuarios que pueden acceder al sistema.
KAWAC en implementación	Solución tecnológica para la administración y el mantenimiento de sistemas de gestión basados en los estándares ISO 9001, ISO 14001, ISO 27001, ISO 31000, OHSAS 18001, RSE, GP1000 y MECI. Esta solución está diseñada para generar un cambio en la cultura de la gestión y para hacer más sencillo el manejo de los sistemas de gestión
SAITH	Sistema que permite el registro Público de Inscripción en Carrera administrativa, registro de Licencias y comisiones especiales (despacho), registro de candidatos para un ascenso (postulados), Crear los aspirantes a ingresar a la FGN, registro de resultados de estudios de seguridad, registro de resultados de pruebas psicológicas, consulta de hojas de vida, reporte de Extracto de hoja de vida
AVE- AMBITO VIRTUAL DE EDUCACIONY FORMACION	Apoya la ejecución del Plan Institucional de Formación y Capacitación de los funcionarios de la Fiscalía.
SATELITE	Bitácora de CTI, en la cual se registran las llamadas que llegan a satélite y verificar si las personas que llaman son realmente

	funcionarios, además verifican vehículos y armas registradas en el SIAF.
CODIS	Es el acrónimo de Combined DNA Index System o sistema indexado combinado de ADN, BANCO DE DATOS DE PERFILES GENÉTICOS. Permite el almacenamiento de perfiles genéticos procesados en el Grupo Genética DNCTI, con fines principalmente de Identificación de personas desaparecidas. Tenemos conectividad con INML
AFIS	El sistema Afis en el pilar fundamental en la aplicabilidad de la biometría para la individualización de los ciudadanos. La biometría es una tecnología de identificación que mide e identifica alguna característica morfológica que diferencia a una persona de otra. Las huellas dactilares son el elemento más común utilizado para realizar identificación biométrica.
ARGIS	ArcGIS es el nombre de un conjunto de productos de software en el campo de los Sistemas de Información Geográfica o SIG. Producido y comercializado por ESRI, bajo el nombre genérico ArcGIS se agrupan varias aplicaciones para la captura, edición, análisis, tratamiento, diseño, publicación e impresión de información geográfica. Estas aplicaciones se engloban en familias temáticas como ArcGIS Server, para la publicación y gestión web, o ArcGIS Móvil para la

	captura y gestión de información en campo.
	ArcGIS Desktop, la familia de aplicaciones SIG de escritorio, es una de las más ampliamente utilizadas, incluyendo en sus últimas ediciones las herramientas ArcReader, ArcMap, ArcCatalog, ArcToolbox, ArcScene y ArcGlobe, además de diversas extensiones. ArcGIS for Desktop se distribuye comercialmente bajo tres niveles de licencias que son, en orden creciente de funcionalidades (y coste): ArcView, ArcEditor y ArcInfo.
SCB	Sistema de información de Balística
SIJUR	Sistema de Información de Control de Procesos. Apoyo a la gestión de la Oficina Jurídica.
SIRCE	Sistema de Información de Control de Procesos Disciplinarios
PROGASIG	Programa de asignación de procesos de ley 600

En este dominio se encuentran los siguientes ámbitos:

5.3.4.1 Ámbito Planeación y Gestión de los Sistemas de Información

Con este ámbito se busca una adecuada planeación y gestión de los sistemas de información (estratégicos, misionales, de apoyo, seguimiento y control). Los lineamientos son los siguientes:

- Definición estratégica de los sistemas de información: La subdirección de las TICs debe definir la arquitectura de los sistemas de información teniendo en cuenta las relaciones entre ellos y la articulación con otros dominios del marco de referencia de AE.

- Directorio de los sistemas de información: La FGN debe disponer de un directorio actualizado de los sistemas de información donde se incluya sus atributos relevantes. Así mismo la entidad es responsable de definir su nivel de acceso a dicho directorio de acuerdo con la normatividad vigente.

  Un modelo para la elaboración del directorio detallado de los sistemas de información se plantea de la siguiente forma:

PLANEACION DE LOS SISTEMAS DE INFORMACION - FGN	
ATRIBUTO	**DESCRIPCIÓN**
Nombre del SI	
Categoría	Estratégico-Misional-Apoyo- Seguimiento y Control
Tipo	Web con base de datos central Cliente servidor BD y scripts Hoja de cálculo
Proveedor	Nombre del servidor/funcionario, contratista o empresa contratista que brinda soporte
Estado	Adquisición, suministro, desarrollo, operación y mantenimiento
N° de licenciamiento y tipo	Licenciamiento ilimitado. Licenciamiento para un procesador. Cantidad de licencias por usuario nombrado. Cantidad de licencias por usuario concurrente.
Fecha de vencimiento licenciamiento	Va de acuerdo con el contrato de mantenimiento y soporte - proveedor
Plataforma de Aplicaciones	Java, Net, PHP, etc

Ubicación servidor de aplicaciones	Ubicación de los servidores de aplicaciones por ambiente, indicando el centro de datos y la ip
Plataforma de Base de Datos	Indique la marca de la base de datos y la versión.(Oracle, MySQL, IBM, etc
Ubicación Base de Datos	Ubicación de la base de datos del aplicativo por ambiente, indicando el centro de datos y la ip.
Responsables de las BD	Datos de contacto de la persona responsable de la base de datos: Nombres y apellidos, correo electrónico, celular, teléfono residencia, cargo.

Así mismo a continuación se muestra el artefacto para portafolio de proyectos de los sistemas de información:

PORTAFOLIO SISTEMAS DE INFORMACION - FGN	
ATRIBUTO	**DESCRIPCIÓN**
Sistema	Nombre del sistema de información de acuerdo con los estándares de la entidad.
Descripción	Descripción del sistema de información de acuerdo a la categoría.
Alcance	Alcance del proyecto (tiempo - costo - alcance)
Necesidades de Negocio	Necesidades de negocio que busca satisfacer el proyecto.
Fecha de Inicio	Fecha establecida como inicio del proyecto
Fecha de Finalización	Fecha establecida como finalización del proyecto

Criterios de éxito	Indicar qué condiciones se deben cumplir para considerar que la implementación del proyecto fue exitosa.
Riesgos inherentes	Riesgos identificados sin implementación de los controles
Riesgos Residuales	El resultado después de aplicar los controles
Análisis de brechas	Comparar el estado y desempeño real en la entidad.

- Arquitectura de referencia de los sistemas de información: la subdirección de las TICs es responsable de definir y hacer evolucionar el diseño de cualquier arquitectura de solución.

- Arquitectura de solución de sistemas de información: La subdirección de las TICs debe definir una arquitectura de solución para cada uno de los proyectos de sistemas de información.

- Metodología de referencia para el desarrollo de sistemas de información: La subdirección de las TICs debe contar con una metodología de referencia que defina los componentes principales de un proceso de desarrollo de software. Las metodologías de referencia deben dar cobertura a todas las soluciones de software de los sistemas de información que la fiscalía construya o adapte. (Se deben incorporar las mejores prácticas de la industria)

- Derechos patrimoniales sobre los sistemas de información: Aplica cuando se suscriban contratos con terceras partes bajo la figura de obra creada por encargo, cuyo alcance incluya el desarrollo de elementos de software, el

autor o autores de la obra debe transferir a la FGN loa derechos patrimoniales sobre los productos.

5.3.4.1.1 Evidencias o soportes de la implementación

Las evidencias de cumplimiento para los lineamientos de este ámbito son:

- Documento u artefacto que describa la arquitectura de los sistemas de información, esta descripción se hace por medio de una ficha técnica (catálogo de los sistemas de información).

- El Catálogo de los sistemas de información (inventario) se tiene publicado en un repositorio o un sitio web donde los interesados tienen acceso.

- Para la arquitectura de referencia y solución de los sistemas de información la entidad a través de la Resolución 0-1261 del 2014 estableció las directrices y buenas prácticas para el desarrollo, mantenimiento y calidad de los sistemas de información.

- Para la metodología de referencia para el desarrollo de sistemas de información, la FGN en la Resolución 0-1261 del 2014 en el capítulo II describe las buenas prácticas para las fases y el ciclo de vida de desarrollo del software.

- En los casos que aplique derechos patrimoniales sobre los sistemas de información, la FGN a través de los contratos de cesión de derechos para los proyectos liquidados y los que se encuentran en curso se evidencian la cesión de los derechos de parte del proveedor. Dicho contrato es radicado ante la Dirección Nacional de Derechos de Autor.

5.3.4.1.2 Roles y Responsabilidades:

Responsable del desarrollo y despliegue de los sistemas de información – Jefe de arquitectura de negocio de la FGN.

Responsable planeación y ejecución de pruebas – Jefe de arquitectura de negocio de la FGN.

Responsable Gestión de Proyectos – Gestor de proyectos en la Fiscalía.

Responsable análisis y generación de la información – Jefe dpto. Sistemas de información en la Fiscalía.

Responsable Aseguramiento de la Calidad – Asesor de procesos y aseguramiento de la calidad en la Fiscalía.

Responsable Administración de cambios – Asesor de procesos y aseguramiento de la calidad en la Fiscalía.

5.3.4.2 Ámbitos Diseño, Ciclo de Vida, Soporte, Gestión de la Calidad y Seguridad de los Sistemas de Información

Con estos ámbitos la entidad contará con sistemas de información estandarizados, interoperables y usables.

Así mismo la entidad buscará definir y gestionar las etapas que deben surtir los Sistemas de Información desde la definición de requerimientos hasta el despliegue, puesta en funcionamiento y uso. Definiendo los aspectos necesarios para garantizar la entrega, evolución y adecuado soporte de los Sistemas de Información. Donde deberá definir y gestionar los controles y mecanismos para alcanzar los niveles requeridos de seguridad, privacidad y trazabilidad de los Sistemas de Información.

Los lineamientos establecidos para estos ámbitos son los siguientes:

- Guía de estilo y usabilidad: Para los sistemas de información que involucren interacción con el ciudadano, deben cumplir con los lineamientos de Gobierno en Línea. El documento debe contar con manejo de versiones, pues estos lineamientos están en constante evolución y se deben ir adaptando con las arquitecturas de referencia y buenas prácticas de la industria. La subdirección de las TICs debe definir una guía de estilo y usabilidad única, que establezca los principios para el estilo de los componentes de presentación, estructura para la visualización de la información y procesos de navegación entre pantallas, entre otros. Esta guía de estilo y usabilidad debe estar particularizada para cada medio tecnológico o canal utilizado por los sistemas de información y, así mismo, debe estar alineada con los principios de usabilidad definidos por el Estado colombiano.

- Apertura de datos, interoperabilidad, implementación de componentes de información, y accesibilidad : La subdirección de las TICs debe habilitar en sus sistemas de información aquellas características funcionales y no funcionales, necesarias para la apertura de sus datos, para interactuar con la Plataforma de Interoperabilidad del Estado colombiano, partiendo de los flujos de información registrados en el directorio de Componentes de información y las necesidades de intercambio de información con otras instituciones. Los sistemas de información deben funcionar sobre la Arquitectura de información definida para la FGN y debe dar soporte a los componentes de información allí incluidos. Los sistemas de información que estén dispuestos para el acceso a usuarios externos o grupos de interés deben cumplir con las características de accesibilidad que indique la estrategia de Gobierno en Línea.

- Ambientes independientes en el ciclo de vida de los sistemas de información: La subdirección de las TICs debe disponer de ambientes independientes y

controlados destinados para desarrollo, pruebas, operación, certificación y capacitación de los sistemas de información, y debe aplicar mecanismos de control de cambios de acuerdo con las mejores prácticas.

- Análisis de requerimientos, Integración continúa durante el ciclo de vida, Plan de pruebas durante el ciclo de vida, Plan de capacitación y entrenamiento, Manual del usuario, técnico y de operación de los sistemas de información: La subdirección de las TICS debe aplicar un proceso formal de manejo de requerimientos, que incluya la identificación, la especificación y el análisis de las necesidades funcionales y no funcionales, la definición de los criterios de aceptación y la trazabilidad de los requerimientos a través del ciclo de vida de los sistemas de información. Debe diseñar e implementar estrategias que permitan la integración continua e incremental de los nuevos desarrollos y que apoyen la automatización de las actividades en las diferentes fases del ciclo de vida de los sistemas de información. Debe contar con un plan de pruebas que cubra lo funcional y lo no funcional. Debe contar con planes de capacitación y entrenamiento a los usuarios, que faciliten el uso y apropiación de los sistemas de información. Debe asegurar que todos sus sistemas de información cuenten con la documentación de usuario, técnica y de operación, debidamente actualizada, que asegure la transferencia de conocimiento hacia los usuarios, hacia la Subdirección de las TICs.

- Actualización y requerimientos de cambio de los sistemas de información: La subdirección de las TICs, debe formalizar la petición de nuevas funcionalidades o de cambios a las existentes, a través de un procedimiento de control de cambios.

- Estrategias de mantenimiento de los sistemas de información: La subdirección de las TICs, debe hacer un análisis de impacto ante un cambio

o modificación de los componentes para determinar las acciones a seguir, por otra parte cuando el mantenimiento es con terceras partes que tienen contratados, la subdirección de las TICs, debe establecer acuerdos de nivel de servicio (ANS) los cuales se validan al inicio del contrato y se define un periodo de transición para empezar aplicar los mismos.

- Plan de calidad, criterios no funcionales, seguridad, privacidad, auditoria y trazabilidad de los sistemas de información: La subdirección de las TICs, dentro de sus planes de desarrollo de sistemas de información debe contar con planes de calidad los cuales deben contar con un repositorio documental validados y aprobados, así mismo para el diseño de los sistemas de información se debe tener en cuenta los requerimientos de la entidad, las restricciones funcionales, técnicas y atributos de calidad, también se deben incorporar componentes de seguridad para el tratamiento de la privacidad de la información, logrando la implementación de controles de acceso, mecanismos de integridad y cifrado de información y se deben tener en cuenta mecanismos que aseguren el registro histórico para poder mantener la trazabilidad de las acciones realizadas por los usuarios.

5.3.4.2.1 Evidencias o soportes de la implementación

- Los sistemas de Información de la entidad que aplican la guía de estilo y usabilidad.

- Conjunto de datos abiertos generados a partir de los procesos automatizados de la entidad y de acuerdo con los criterios de calidad de la guía de apertura de datos de gobierno en línea.

- Servicio habilitado y funcionando en la Plataforma de Interoperabilidad del Estado colombiano.

- Matriz de correlación entre los componentes de información y los sistemas de información de la entidad.

- Plan de pruebas que incorpore un criterio de aceptación para accesibilidad de acuerdo a la caracterización de usuarios realizada sobre el sistema.

- La entidad debe evidenciar la existencia, durante el ciclo de vida de los sistemas de información, de ambientes independientes y controlados. Se recomienda que este ambiente este conformado por los siguientes elementos: código fuente, configuración del ambiente, ID – Entorno de desarrollo, documentación, manuales de instalación, definición de roles y responsabilidades, copias de sus ambientes para utilizar a futura para actualizaciones, esquema de operación y control de cambios donde se especifique un protocolo de paso de versiones entre ambientes.

- La entidad definirá una metodología para el desarrollo de los sistemas de información y dentro de la fase de gestión de requerimientos se debe definir y detallar lo siguiente: identificación, levantamiento, análisis, validación y trazabilidad de los requerimientos, así mismo se deben incluir actividades o procedimiento de integración continua, como también deben estar incluidos los planes de pruebas funcionales. Lo anterior debe ser socializado con todos los involucrados tanto al interior de la entidad como con los proveedores.

- Dentro de los planes de proyectos de desarrollo de sistemas de información se debe contar con planes de capacitación y entrenamiento que faciliten el uso y apropiación de los mismos.

- Se deben definir entregables del producto, la documentación de usuario, técnica y de operación necesaria para cada sistema de información.

- La entidad debe formalizar un procedimiento documentado para la gestión de cambios. (La FGN actualmente cuenta con el proceso de gestión integral, que dentro de sus funciones está la de control de cambios). Por otra parte los ANS para la prestación de servicios de mantenimiento por terceros para los sistemas de información estos deben ser validados desde el inicio del contrato.

- Para los planes de calidad debe considerarse lo siguiente: alcance, objetivos, responsables, actividades, estrategias de ejecución del plan de calidad, como se va a ejecutar el plan y como validar su ejecución (métricas e indicadores, cronograma de actividades, validaciones periódicas, mecanismos de control, en este documento se debe incluir las restricciones funcionales y técnicas de las arquitecturas de referencia.

- Para los componentes de seguridad se deben implementar los establecidos en el modelo de seguridad y privacidad de la información establecida por MINTIC. Así mismo para la auditoria y trazabilidad los logs de trazas evidencian las acciones realizadas por los usuarios.

5.3.4.2.2 Roles y Responsabilidades:

Los mismos que se describen en el punto **5.3.4.1.2** de este documento.

5.3.5 DOMINIO SERVICIOS TECNOLOGICOS – APLICADO A LA ENTIDAD DE CONTROL (FGN)

Este dominio permite a la entidad gestionar con mayor eficacia y transparencia la infraestructura tecnológica que soporta los sistemas y servicios de información. Dentro de este dominio se encuentran los siguientes ámbitos:

5.3.5.1 Ámbitos Arquitectura, Operación, Soporte, Gestión de la Calidad y Seguridad en los Servicios Tecnológicos.

Estos ámbitos tienen como función apoyar a la subdirección de la TICs con los lineamientos y estándares orientados a la definición y diseño de la Arquitectura de infraestructura tecnológica que se requiere para soportar los sistemas de información y el portafolio de servicios, donde se implementen procesos de operación, monitoreo y supervisión, con el fin de gestionar adecuadamente los procesos de soporte y mantenimiento de los servicios tecnológicos. Y por último busca la definición y gestión de los controles y los mecanismos para alcanzar los niveles requeridos de seguridad y trazabilidad de los servicios tecnológicos.

Los lineamientos que hacen parte de estos ámbitos son los siguientes:

- Directorio de servicios tecnológicos: directorio donde se describan todos los servicios de la entidad.

- Elementos para el intercambio de información: la entidad debe asegurar el cumplimiento de la ICDE de tal forma que permita el intercambio de información geo-espacial y georreferenciada.

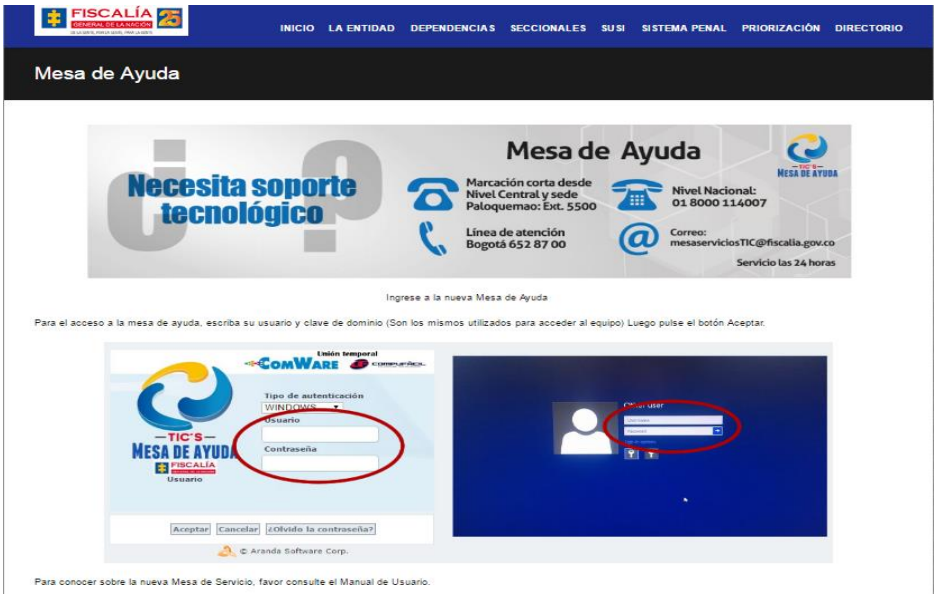
- Gestión de los servicios tecnológicos: se debe gestionar la estabilidad de TI

- Acceso a servicios en la nube: N/A para la FGN

- Tecnología verde: En la FGN se tienen implementado este proyecto con el nombre de justicia verde.

- Continuidad, disponibilidad y capacidad de los servicios tecnológicos: la subdirección de las TICs debe garantizar que sus servicios tecnológicos estén respaldados con sistemas de alimentación eléctrica, mecanismos de refrigeración, soluciones de detección de incendios, sistemas de control de accesos y sistemas de monitoreo de componentes físicos que aseguren la continuidad y disponibilidad del servicio. Asi mismo la subdirección de las TICs debe identificar las capacidades actuales de los servicios de TI, identificando las capacidades actuales de los servicios tecnológicos y proyectando las capacidades futuras requeridas para que cumplan con los niveles de servicios acordados.

- Acuerdos de Niveles de servicios, Mesa de ayuda y planes de mantenimiento: Actualmente la FGN cuenta con acuerdos de niveles de servicios ANS de acuerdo con contrato suscrito con la empresa unión temporal COMWARE – COMPUFACIL, estos son manejados a través de la mesa de ayuda de la entidad, según se muestra a continuación:



FUENTE: MESA DE AYUDA DE LA FGN

RUTA INTERNA: http://web.fiscalia.col/fiscalnet/mesa-de-ayuda-2/

- A través de la mesa de ayuda se aplica el procedimiento de atención de requerimientos de TI, así mismo se realiza reporte e informes de los mantenimientos realizados.

- Control se recursos compartidos, gestión preventiva de servicios, respaldo y recuperación de los servicios tecnológicos: La subdirección de las TICs debe identificar, monitorear y controlar el nivel de consumo de los recursos críticos que son compartidos por los servicios tecnológicos. Así mismo se debe contar con un proceso periódico de respaldo de la configuración de los servicios tecnológicos.

- Análisis de vulnerabilidades, monitoreo de seguridad de infraestructura tecnológica: La subdirección de las Tics a través de un plan de pruebas debe

identificar y tratar los riesgos que puedan comprometer la seguridad de la información o que pueda afectar la prestación del servicio de TI.

5.3.5.2 Evidencias o soportes de la implementación

- Directorio de servicios tecnológicos incluidos los servicios por terceros.

- Diagrama arquitectónico que representen los elementos de infraestructura involucrados en el intercambio de información al interior de la entidad y con sistemas externos.

- Implementación de mecanismos de Rollback en caso de fallos en el despliegue, definición de ventanas de mantenimiento, ambientes independientes, pruebas necesarias y demás actividades encaminadas en minimizar los riesgos de caída del sistema de producción.

- Para el lineamiento relacionado con tecnología verde la entidad lo tiene bajo el tema de justicia verde así:

FUENTE: INTRANET DE LA FGN

RUTA INTERNA: http://web.fiscalia.col/fiscalnet/

Así mismo la subdirección de las TICs tiene las siguientes políticas para este tema:

- Guía para ahorro de tóner tinta para impresoras.
- Uso eficiente del papel, por lo que se tienen habilitado el uso de papel reciclable.
- Teleconferencias a Nivel Nacional
- Control del consumo de electricidad (mensualmente se verifican los pagos realizados por este concepto a través de los informes de austeridad en el gasto realizado por los auditores seccionales).
- Todas las seccionales manejan la centralización de los sistemas de impresión.
- El reciclaje de los equipos de TI en las seccionales se realiza a través del procedimiento de bajas establecido por la entidad (Resolución 0-0532 del 02/04/2014)
- Centralización del almacenamiento de datos (todos los datos son centralizados en Bogotá – NC).
- Para la continuidad y disponibilidad de los servicios tecnológicos la FGN tiene implementado planes, procedimientos, políticas y sistema de respaldo a través de un sitio alterno para el manejo de los sistemas de información más críticos. Es así como se deben tener en cuenta lo siguiente:
    - ✓ Establecer las políticas y alcance

- ✓ Evaluar el impacto en el negocio de una interrupción de los servicios TI
- ✓ Analizar y prever los riesgos a los que está expuesto la infraestructura TI
- ✓ Establecer las estrategias de continuidad del servicio TI
- ✓ Adoptar medidas proactivas de prevención del riesgo
- ✓ Desarrollar los planes de contingencia
- ✓ Poner a prueba dichos planes
- ✓ Formar al personal sobre los procedimientos necesarios para la pronta recuperación del servicio
- ✓ Revisar periódicamente los planes para adaptarlos a las necesidades reales del negocio.

5.3.5.3 Roles y Responsabilidades:

Responsable del dominio de Servicios tecnológicos es el subdirector de las TICs.

5.3.6 DOMINIO USO Y APROPIACIÓN – APLICADO A LA ENTIDAD DE CONTROL (FGN)

Este dominio define lineamientos orientados a lograr el involucramiento de los diversos procesos existentes en la entidad en la participación de las iniciativas de TI, y el desarrollo de competencias TI. El Uso y Apropiación de TI es el resultado de un esfuerzo de transformación eficiente, direccionado por lineamientos, estándares y guías; los cuales se expresan en el presente dominio.

5.3.6.1 Ámbitos y lineamientos de este dominio

LINEAMIENTOS ASOCIADOS AL DOMINIO DE USO Y APROPIACIÓN	
AMBITOS	**LINEAMIENTOS**
ESTRATEGIAS PARA EL USO Y APROPIACION DE TI	**Estrategia de uso y apropiación** Documento de la estrategia el cual debe contener lo siguiente: **1-** Proyectos e iniciativas para la movilización de los grupos de interés en favor de las iniciativas de TI. **2-** Desarrollar competencias de TI en los servidores de la FGN. **3-** implementar indicadores de uso y apropiación que permitan evaluar el nivel de adopción de TI, actividad que desarrollara la DCI y de acuerdo con las recomendaciones emitidas elaborar plan de mejoramiento. **4-** Evidencias de ejecución: correos institucionales enviados a los servidores y funcionarios de la FGN comunicando la existencia de la estrategia de uso y apropiación de la entidad. Listado de asistencia y fotografías jornadas de capacitación y/o presentación de la estrategia a los servidores de la FGN. Concursos, enlaces de publicación en la intranet, protectores de pantalla, carteleras informativas digitales.
	Matriz de interesados Matriz de caracterización del proceso de Gestión de TI con la priorización de los grupos de interés (internos y externos)
	Involucramiento y compromiso Estrategias de sensibilización según grupos de interés, teniendo en cuenta el tipo de seccional: A - B - C. Tipo A: Cuenta con Dirección y 4 subdirecciones (SAG, SSFS,SPJCTI,SSAVU), Tipo B: cuenta con Dirección y 3 subdirecciones (SAG, SSFS,SPJCTI), tipo C: cuenta con 3 subdirecciones (SAG, SSFS,SPJCTI)

	Esquema de Incentivos Diseñar un esquema de incentivos(no monetarios) por cada Dirección Nacional para quienes demuestren uso y aprovechamiento de las TI, por ejemplo: reconomiento de LOW MULTRA, accensos, diplomados, etc.
	Plan de formación Documento en el cual se muestra el plan de formación y capacitación para los servidores de la entidad (para cada vigencia uno) y la Dirección de control interno verificar el cumplimiento a traves de informes trimestrales a la Dirección Nacional de Apoyo a la Gestión.
GESTION DEL CAMBIO DE TI	**Preparación para el cambio** Procedimiento documentado de la gestión del cambio.
	Evaluación del nivel de adopción de TI Formulación de indicadores de adopción de la tecnología y la satisfacción de su uso.
	Gestión de impactos Documento de plan de gestión de impactos establecidos y aprobados mediante acto administrativo en la FGN.
MEDICION DE RESULTADOS EN EL USO Y APROPIACION	**Sostenibilidad del cambio** Documentos de la sostenibilidad del cambio en el cual se realiza el plan para la transferencia del conocimiento a los nuevos servidores y/o funcionarios, con el fin de cumplir con el direccionamiento estratégico vigente.
	Acción de Mejora Documento con la descripción de las acciones de mejora en procura de mejorar los indicadores de uso y apropiación de los proyectos e iniciativas de TI.

5.3.6.2 Roles y Responsabilidades:

Responsable del dominio de Uso y apropiación es la Dirección Nacional de Apoyo a la Gestión, líderes de calidad de cada uno de los procesos de la entidad, apoyo y asesoría de la Dirección de Control interno para las sensibilizaciones a los grupos de interés.

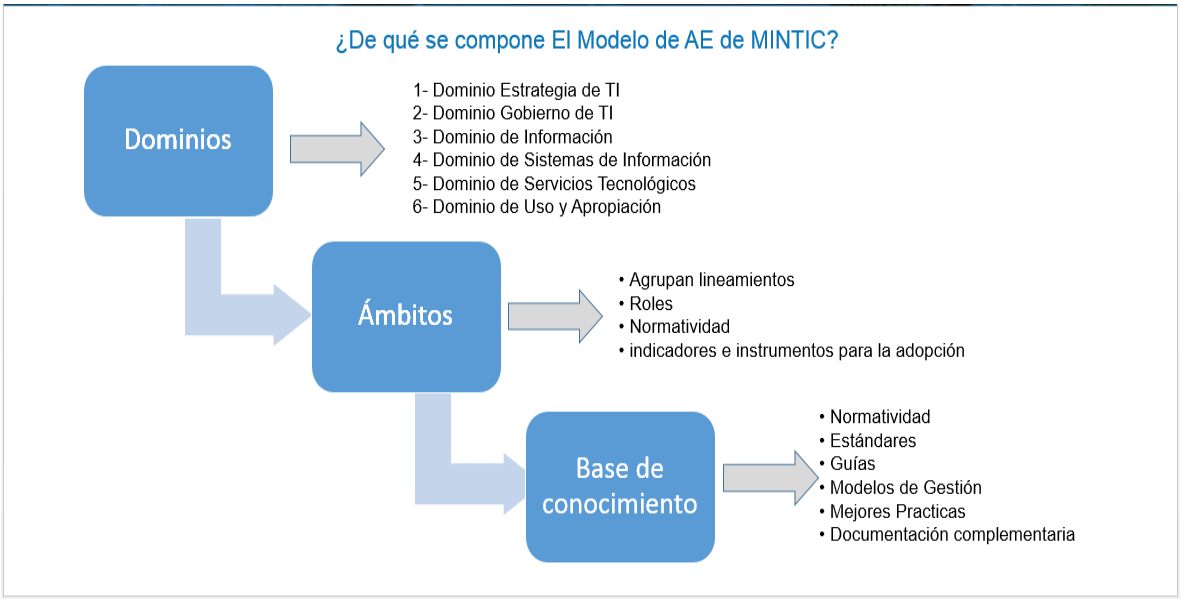
FASE IV. PRESENTACION DE LA PROPUESTA

Esta propuesta será presentada al señor Fiscal General de la Nación a través de un brochure de forma digital e impresa.

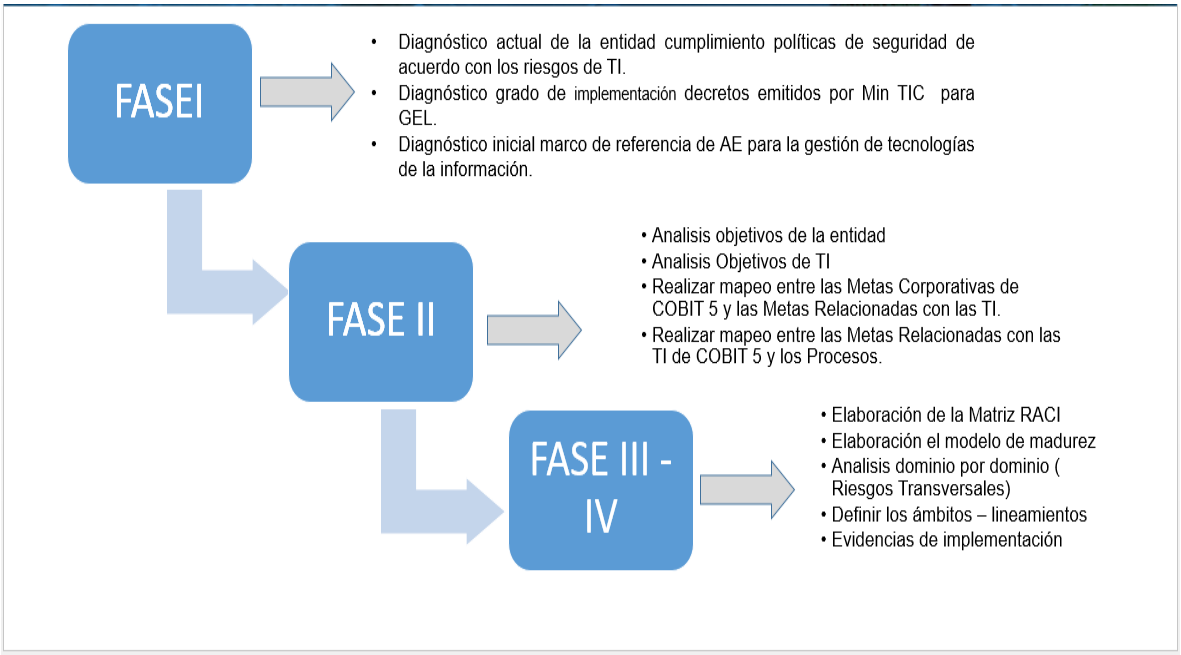
El brochure será presentado a los jurados al momento de la sustentación del proyecto. (El brochure que se presentará a los jurados no llevará el logo de la entidad por protocolos de seguridad internos de la FGN y evitar posibles sanciones disciplinarias y penal de las autoras del proyecto).

A continuación se establece un resumen de los pasos para la implementación de AE en una entidad de control, teniendo como base la gestión de Riesgos transversales en cada dominio:

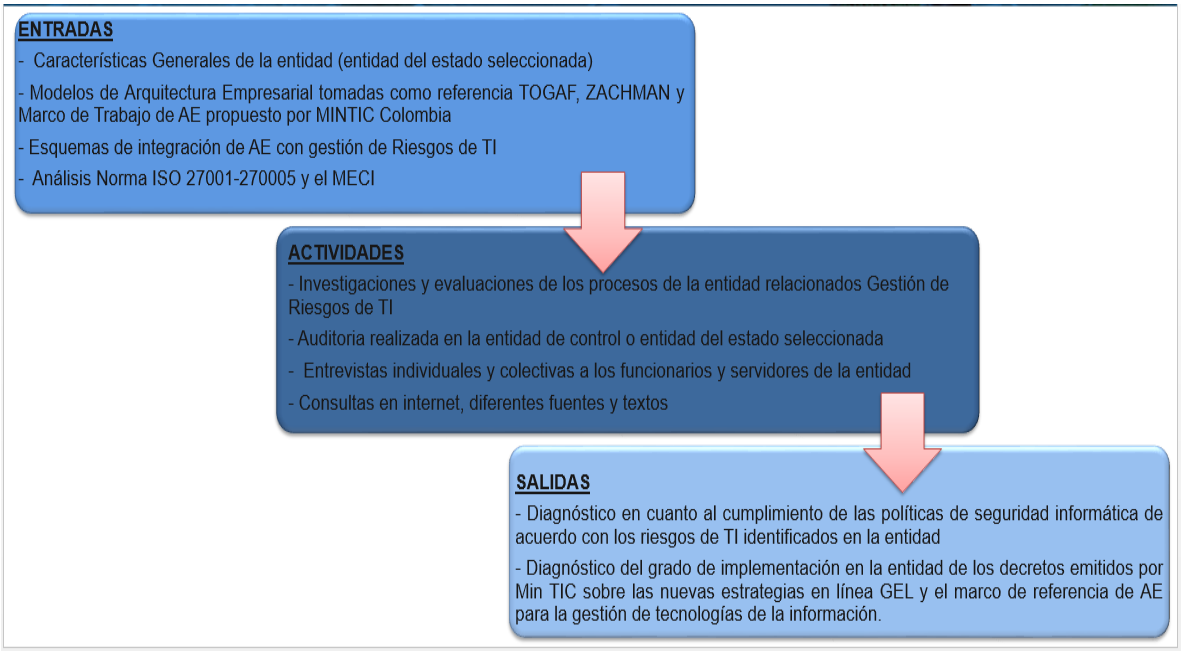
¿De qué se compone El Modelo de AE de MINTIC?



¿Cuáles son los Componentes de la Guía Propuesta?



¿Qué contiene la fase I – Diagnóstico de la entidad de control?



Diagnóstico de la Cadena Valor Actual Vs Cadena de Valor Deseada

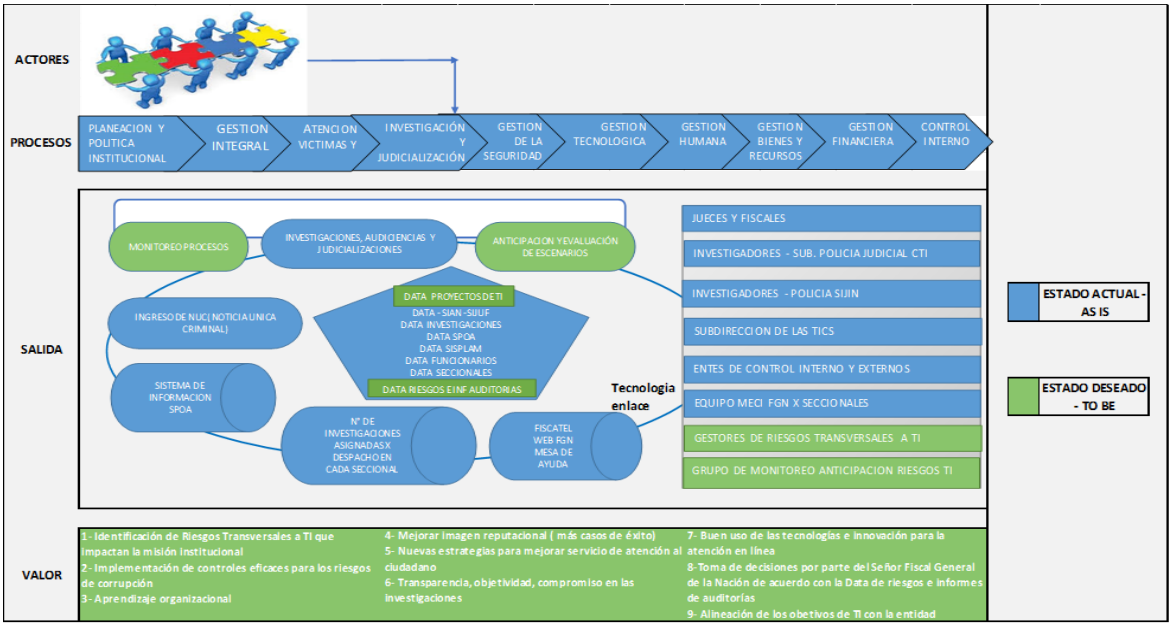


Figura 23: Estado Actual Vs Deseado de la Entidad de control

Fuente: iniciativa propia

Modelo de Gobierno y de Gestión de TI en la entidad (Arquitectura de Negocio)

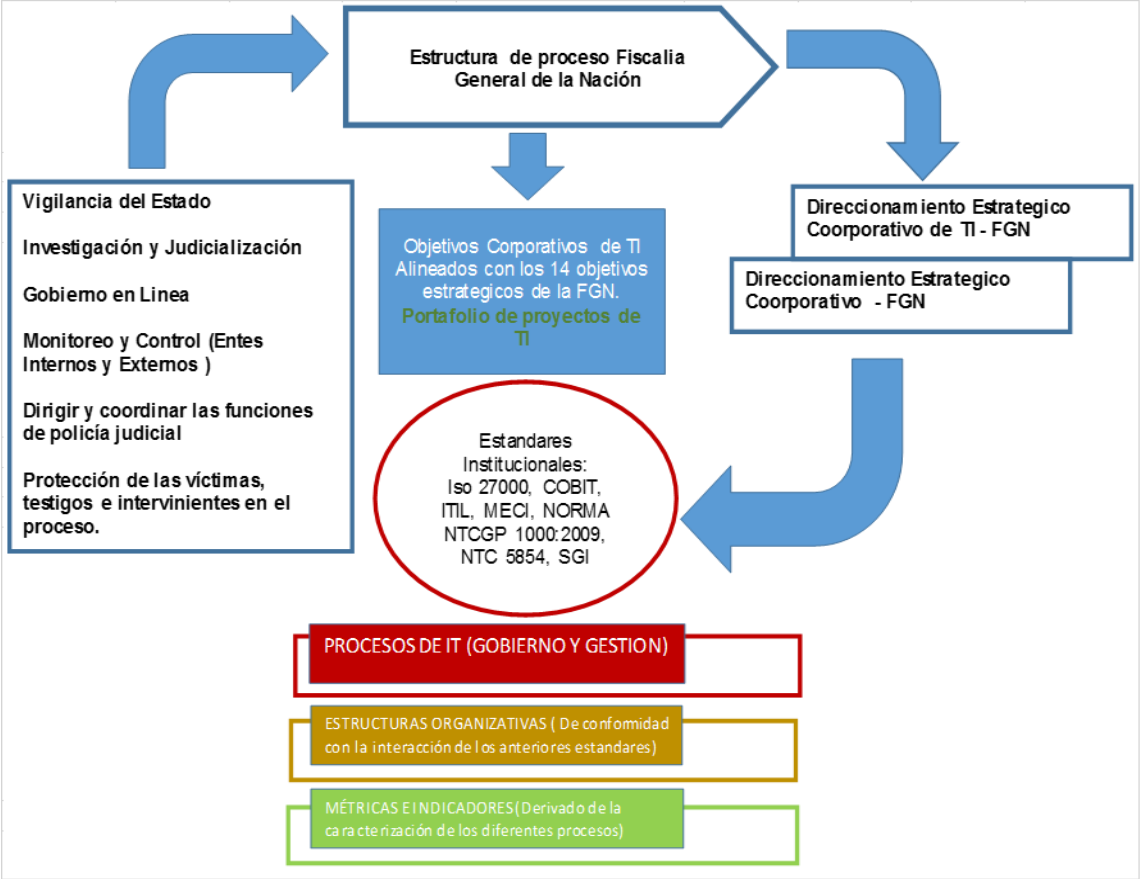


Figura 24: Modelo G. y G de TI en la entidad de control

Fuente: Iniciativa propia

Se seleccionan los principales Procesos de COBIT 5.0 Para Aplicar en la entidad, para la entidad de control en estudio se seleccionaron los siguientes:

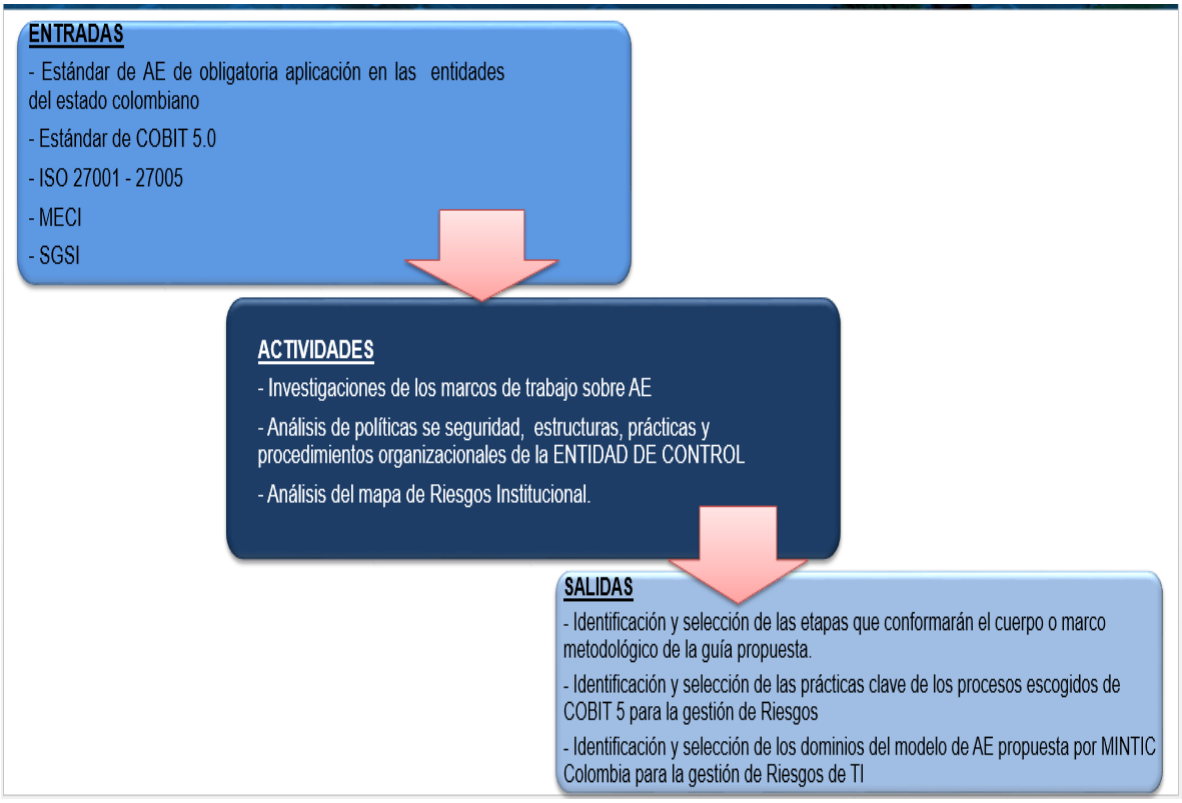
APO03: Gestionar la Arquitectura Empresarial

APO12: Gestionar el Riesgo

DSS06: Gestionar los controles de los procesos del negocio

MEA03: Supervisar, evaluar y valorar la conformidad con los requerimientos externos.

¿Qué contiene la fase II?



A partir de los procesos seleccionados por la entidad de control (COBIT 5.0) en la fase I, se procede a realizar la matriz RACI y la línea de madurez para cada uno de los procesos seleccionados, a continuación se muestra ejemplo de la matriz RACI y la línea de madurez para el proceso **APO03** seleccionado para este caso de estudio.

MATRIZ RACI APO03- APLICADO A LA ENTIDAD (F.G.N.)

MATRIZ RACI APO03 - FISCALIA GENERAL DE LA NACION																											
PRACTICA CLAVE DE GOBIERNO	PRESIDENTE COLOMBIA	FISCAL GENERAL DE LA NACION (CEO)	VICEFISCAL (CFO)	DIRECTOR NACIONAL DE APOYO A LA GESTION (COO)	SUBDIRECCION FINANCIERA	LIDERES DE LOS PROCESOS (DIRECTORES OFICINAS)	DIRECCION NACIONAL DE POLITICAS PUBLICAS Y DE PLANEACION	DIRECCION NACIONAL DE ESTRATEGIAS CONSTITUCIONALES	GESTOR DE PROYECTOS	OFICINA GESTIÓN DEL VALOR	DIRECTOR DE RIESGOS (CRO)	DIRECTOR DE SEGURIDAD DE LA INFORMACIÓN (CISO)	DIRECTOR DE ARQUITECTURA EMPRESARIAL	COMITÉ DE RIESGOS CORPORATIVOS	JEFE DE TALENTO HUMANO	DIRECCIÓN JURIDICA (COMPILANCE)	DIRECCIÓN DE CONTROL INTERNO	SUBDIRECTOR DE LAS TICs (CIO)	JEFE ARQUITECTURA DE NEGOCIO	JEFE DPTO INFRAESTRUCTURA TECNOLOGICA	JEFE DPTO SISTEMAS DE INFORMACIÓN	JEFE DE COMUNICACIONES	JEFE DE SEGURIDAD	ASESOR DE PROCESOS Y ASEGURAMIENTO DE LA CALIDAD	JEFE ATENCIÓN REQUERIMIENTOS INFORMATICOS Y	JEFE CONTINUIDAD DE NEGOCIO
APO03.01 - Desarollar la visión de la arquitectura de la Fiscalía General de la Nación		A	C	C	R	C	R					C	R	C	C	C	C	R	R	C	C	C		C		
APO03.02 Definir la arquitectura de referencia establecida para las entidades del estado		C	C	C	R	C	R					C	A	C	C	C	C	R	R	C	C	C		C		
APO03.03 Seleccionar las oportunidades y soluciones		A	C	C	R	C	R					C	R	C	C	C	C	R	R	C	C	C		C		
APO03.04 Definir la implantación de la arquitectura		A	C	R	C	C	R					C	R	C	C	C	C	R	R	C	C	C		C		
APO03.05 Proveer los servicios de AE		A	C	R	C	C	R					C	R	C	C	C	C	R	R	C	C	C		C		

FIG. 25 Matriz RACI – FGN – APO03

Fuente: Iniciativa Propia

	ESTADO ACTUAL -AS IS
	ESTADO DESEADO - TO BE

Línea de Madurez APO03 – Entidad (FGN)

Alinear, Planificar y Organizar

APO03- Establecer una AE en la F.G.N	NIVEL ACTUAL	NIVEL ESPERADO
APO03.01 - Desarrollar la visión de la arquitectura de la Fiscalía General de la Nación	0	2
APO03.02 Definir la arquitectura de referencia establecida para las entidades del estado	1	3
APO03.03 Seleccionar las oportunidades y soluciones	0	3
APO03.04 Definir la implantación de la arquitectura	0	3
APO03.05 Proveer los servicios de AE	0	3

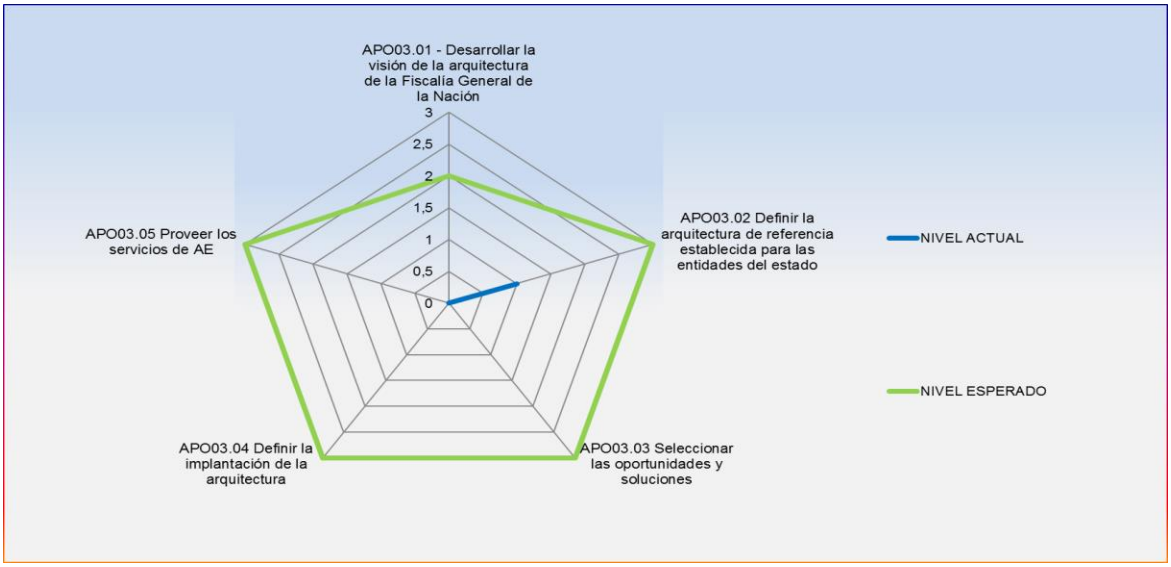
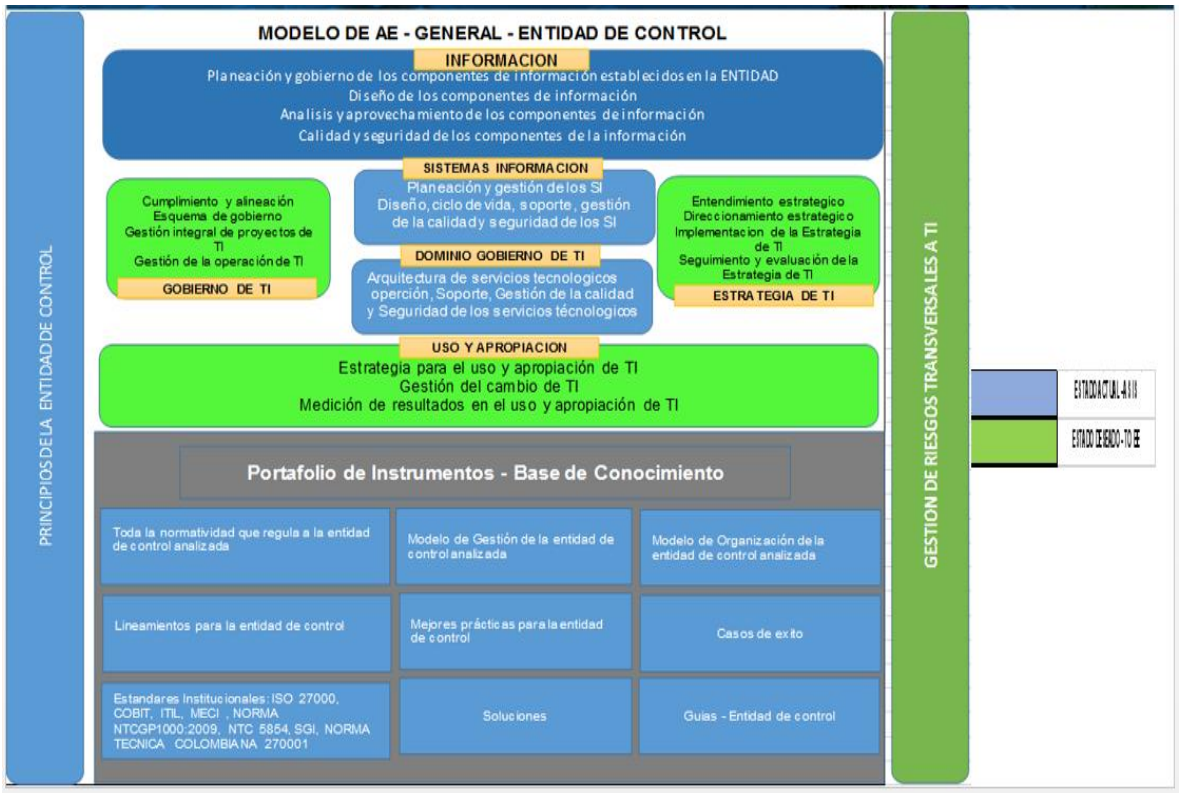


Figura 26: Modelo Madurez APO03-FGN

Fuente: Iniciativa propia

¿Qué contiene la fase III y IV?

El diseño y construcción, que corresponde en aplicar el diseño propuesto por MINTIC a la entidad de control, con el fin de definir las evidencias dominio por dominio para que al momento de realizar seguimientos a su implementación se puedan tener los soportes idóneos de acuerdo con la identificación y gestión de riesgos transversales efectuada en cada uno de los procesos de la entidad.

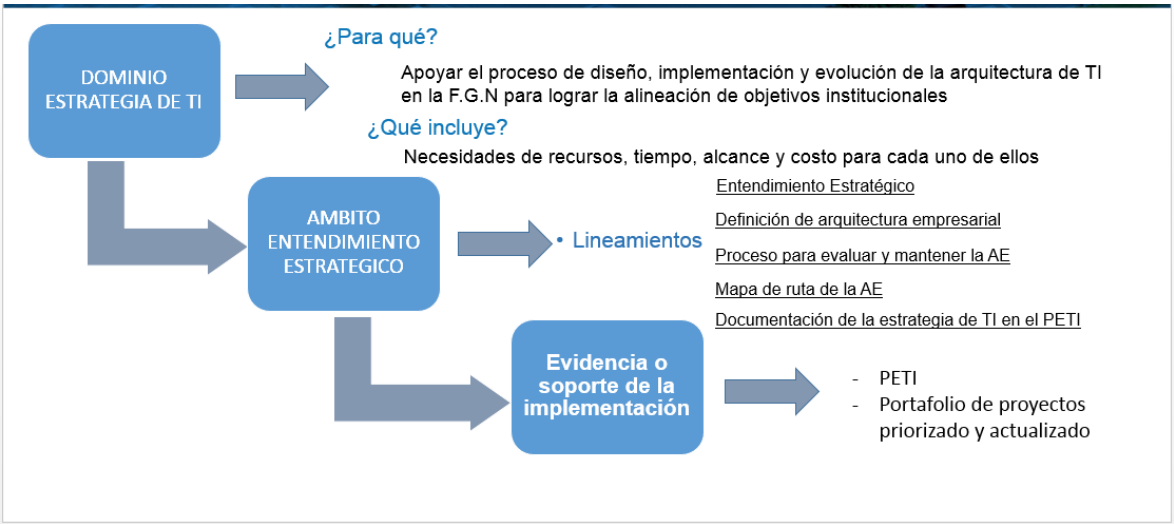


	ESTADO ACTUAL -AS IS
	ESTADO DESEADO - TO BE

Figura 29: Modelo de AE – General para una entidad de control

Fuente: Iniciativa propia y resultado de este trabajo de grado (Complementa la implementación de AE en la FGN) y tomando como base el modelo de AE propuesto por MINTIC

Ejemplo del contenido de la guía para un ámbito de un dominio



CONCLUSION

Tomando como base de estudio una institución del estado como la Fiscalía General de la nación, y analizando los diferentes marcos de trabajo existentes de arquitectura empresarial, se entrega una guía propuesta para implementar Arquitectura empresarial en cualquier entidad de control del estado y poder realizar una gestión estratégica de TI.

Esta guía se logra a partir del análisis del estado actual de la entidad u organización y determinando cuales deberían ser los pasos que se debe realizar en cada uno de los dominios que propone el modelo de Arquitectura empresarial establecida por el MINTIC con sus entradas y salidas definidas, resaltando que los riesgos de TI deben ser transversales a todos los dominios y en todos los procesos existentes en la entidad. Para lograr una alienación eficaz entre los procesos, los datos, las aplicaciones y tecnología con los objetivos estratégicos definidos en la entidad.

REFERENCIAS BIBLIOGRAFICAS CONSULTADAS

[1] Revista Ingenierías Universidad de Medellín, ARQUITECTURA EMPRESARIAL – UNA VISIÓN GENERAL. Martín Darío Arango Serna, Jesús Enrique Londoño Salazar, Julián Andrés Zapata Cortés, vol. 9, No. 16, pp. 101-111 - ISSN 1692-3324 - enero-junio de 2010/174 p. Medellín, Colombia

[2] ISACA. A Business Framework for the Governance and Management of Enterprise IT. USA (2009). Pp. 91.

[3]https://colombiadigital.net/actualidad/articulos-informativos/item/8123-que-es-arquitectura-empresarial.html.

[4]http://www.ibm.com/developerworks/ssa/rational/library/edge/09/jun09/enterprisearchitecture/

[5] http://www.mintic.gov.co/gestionti/615/articles-5322_Revista_pdf.pdf

[6]http://cintel.co/wp-content/uploads/2013/05/por-que-arquitectura-empresarial.pdf

[7] Guía de bolsillo TOGAF V. 9.1.1’

[8] https://chae201521701014974.wordpress.com/2015/11/10/marco-de-trabajo-zachman/

[9] http://www.mintic.gov.co/arquitecturati/630/w3-propertyvalue-8161.html

[10]http://www.mintic.gov.co/gestionti/615/articles4211_sumen_del_diseno_y_especificacion_del_Marco_de_Referencia_de_la_Arquitectura_Empresarial_para_la_Gestion_TI_del_Estado.pdf

[11] http://www.fiscalia.gov.co/colombia/la-entidad/quienes-somos/

[12]http://www.fiscalia.gov.co/colombia/wpcontent/uploads/2012/01/Constitucion_Politica.pdf

[13] http://www.fiscalia.gov.co/colombia/la-entidad/mision/

[14] http://www.fiscalia.gov.co/colombia/la-entidad/vision/

[15] http://web.fiscalia.col/fiscalnet/fiscal-general-de-la-nacion/direccion-de-control-interno/

[16] http://www.fiscalia.gov.co/colombia/wp-content/uploads/DECRETO-016-DEL-09-DE-ENERO-DE-2014.pdf

[17]http://www.fiscalia.gov.co/colombia/wpcontent/uploads/2013/03/DireccionamientoEstrategico2013_2016.pdf

[18] https://www.auditool.org/blog/auditoria-de-ti/297-la-gestion-de-riesgos-de-ti-en-el-marco-corporativo

[19] Manual Técnico del Modelo Estándar de Control Interno para el Estado Colombiano MECI 2014.

[20] Norma Técnica Colombiana NTC-ISO-IEC 27001.

[21] http://tesisdeinvestig.blogspot.com.co/2011/05/tipos-de-investigacion.html

[22] http://www.mintic.gov.co/arquitecturati/630/w3-propertyvalue-8114.html

[23] http://www.mintic.gov.co/portal/604/w3-propertyvalue-558.html

[24] http://insecurityit.blogspot.com.co/2015/07/la-auditoria-de-ti-en-un-entorno-vica.html

[25] http://www.mintic.gov.co/portal/604/w3-article-9290.html

[26] https://es.linkedin.com/pulse/impacto-de-los-capex-y-opex-en-la-gesti%C3%B3n-activos-amendola

[27] http://www.icde.org.co/quienes-somos/que-es-la-icde

[28] http://www.mintic.gov.co/gestionti/615/w3-propertyvalue-6274.html